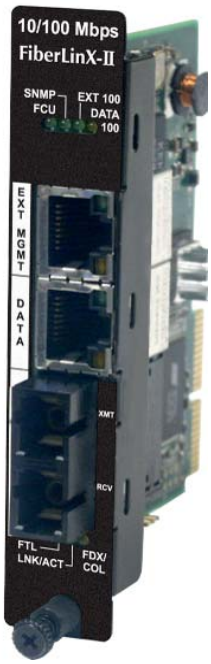
iMcV-FiberLinX-II

Operation Manual



Above illustrations are representative; some minor differences may be present in actual product

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A computing device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The use of non-shielded I/O cables may not guarantee compliance with FCC RFI limits. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Warranty

IMC Networks warrants to the original end-user purchaser that this product, EXCLUSIVE OF SOFTWARE, shall be free from defects in materials and workmanship under normal and proper use in accordance with IMC Networks' instructions and directions for a period of six (6) years after the original date of purchase. This warranty is subject to the limitations set forth below.

At its option, IMC Networks will repair or replace at no charge the product which proves to be defective within such warranty period. This limited warranty shall not apply if the IMC Networks product has been damaged by unreasonable use, accident, negligence, service or modification by anyone other than an authorized IMC Networks Service Technician or by any other causes unrelated to defective materials or workmanship. Any replaced or repaired products or parts carry a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

To receive in-warranty service, the defective product must be received at IMC Networks no later than the end of the warranty period. The product must be accompanied by proof of purchase, satisfactory to IMC Networks, denoting product serial number and purchase date, a written description of the defect and a Return Merchandise Authorization (RMA) number issued by IMC Networks. No products will be accepted by IMC Networks which do not have an RMA number. For an RMA number, contact IMC Networks at PHONE: (800) 624-1070 (in the U.S and Canada) or (949) 465-3000 or FAX: (949) 465-3020. The end-user shall return the defective product to IMC Networks, freight, customs and handling charges prepaid. End-user agrees to accept all liability for loss of or damages to the returned product during shipment. IMC Networks shall repair or replace the returned product, at its option, and return the repaired or new product to the end-user, freight prepaid, via method to be determined by IMC Networks. IMC Networks shall not be liable for any costs of procurement of substitute goods, loss of profits, or any incidental, consequential, and/or special damages of any kind resulting from a breach of any applicable express or implied warranty, breach of any obligation arising from breach of warranty, or otherwise with respect to the manufacture and sale of any IMC Networks product, whether or not IMC Networks has been advised of the possibility of such loss or damage.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, IMC NETWORKS MAKES NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS IMC NETWORKS PRODUCT, INCLUDING WITHOUT LIMITATION ANY SOFTWARE ASSOCIATED OR INCLUDED. IMC NETWORKS SHALL DISREGARD AND NOT BE BOUND BY ANY REPRESENTATIONS OR WARRANTIES MADE BY ANY OTHER PERSON, INCLUDING EMPLOYEES, DISTRIBUTORS, RESELLERS OR DEALERS OF IMC NETWORKS, WHICH ARE

INCONSISTENT WITH THE WARRANTY SET FORTH ABOVE. ALL IMPLIED WARRANTIES INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY LIMITED TO THE DURATION OF THE EXPRESS WARRANTY STATED ABOVE.

Every reasonable effort has been made to ensure that IMC Networks product manuals and promotional materials accurately describe IMC Networks product specifications and capabilities at the time of publication. However, because of ongoing improvements and updating of IMC Networks products, IMC Networks cannot guarantee the accuracy of printed materials after the date of publication and disclaims liability for changes, errors or omissions.

Table of Contents

FCC Radio Frequency Interference Statement ---------- ii
Warranty ---------- ii
About the iMcV-FiberLinX-II ---------- 1
iView^2 Management Software ---------- 4
Installation ---------- 5
  Small Form-Factor Pluggable Ports (SFP) ---------- 5
LED Operation ---------- 6
  TX/FX LEDs ---------- 6
  TX/SFP LEDs ---------- 7
  SFP/SFP LEDs ---------- 8
Hardware Configuration ---------- 9
Software Configuration ---------- 11
Configuration File Save/Restore Function ---------- 12
  Configuration File Basics ---------- 13
  Uploading a Saved Configuration File through iConfig ---------- 15
  Uploading a Saved Configuration File through TFTP ---------- 16
Using Telnet ---------- 22
  Basic Device Configuration ---------- 23
Application Overview ---------- 37
Application Examples ---------- 38
Troubleshooting ---------- 54
Serial Port Pinout ---------- 56
Modes of Operation ---------- 57
Appendix ---------- 58
IMC Networks Technical Support ---------- 59
Specifications ---------- 60
Standards/Compliance ---------- 61
Fiber Optic Cleaning Guidelines ---------- 62
Electrostatic Discharge Precautions ---------- 63
Safety Certifications ---------- 64

About the iMcV-FiberLinX-II

NOTE
Unless noted otherwise, all references to the iMcV-FiberLinX-II in this manual are also applicable to the iMcV-FiberLinX-II TX/SFP and iMcV-FiberLinX-II SFP/SFP.

Overview

The iMcV-FiberLinX-II allows network operators to deploy managed Ethernet services, with a full range of remote management, traffic monitoring, and alarm reporting features. Operators can choose from enhanced versions combining 100 Mbps fiber to 10/100 Mbps copper media conversion, or an all-copper version. The fiber-to-copper versions are available for a range of fiber connectors (SC, ST, or SFP) and a variety of wavelengths, supporting higher density CWDM and single-strand fiber operation.

The iMcV-FiberLinX-II supports two main configuration modes: Standalone or Host/Remote. When using Host/Remote, the Remote modules can be fully managed without an IP address, using a secure management channel. In either mode, the network operator can choose to assign an IP address to the Host or Standalone module. Or, if using a local iMediaChassis managed chassis, all local and remotely connected iMcV-FiberLinX-II modules can be managed using a single IP address (the iMediaChassis IP address). This not only preserves IP addresses and reduces configuration complexity, but management traffic traveling on the non-IP based transmission channel is kept isolated from customer traffic, enhancing network security.

The iMcV-FiberLinX-II offers the following features:

- Securely separates the SNMP management network from the data network
- IEEE 802.1Q VLAN Tagging
- Q-in-Q VLAN Extra-Tagging with EtherType (TPID) selection
- Remote traffic monitoring
- Remote automatic alarms
- Bandwidth limiting
- FiberAlert (loss return)– Fiber versions only
- FX and TX LinkLoss Link: Fault Pass Through (LFPT)
- Loopback testing
- Auto Negotiation
- Selective Advertising
- AutoCross
- Broadcast Storm Protection

The iMcV-FiberLinX-II module is a single-slot chassis-mounted module.

Compatible chassis include the following:

- iMediaChassis series
- MediaChassis series
- IE-MediaChassis series

Port Interfaces

Every iMcV-FiberLinX-II includes the following ports:

- One 10/100 twisted pair (RJ-45) data port
- One additional 10/100 twisted pair port (EXT MGMT) for management (can also function as a serial port)

And one of the following uplink ports:

- One 100 Mbps Fiber
- One additional 10/100 twisted pair (RJ-45)
- One SFP port (requires one SFP/155-ED Module)

Configure the iMcV-FiberLinX-II by using either the serial craft port connection, or a SNMP management application such as iView^2 or a Telnet session.

About Serial Port Configuration

The iMcV-FiberLinX-II includes a serial port on the unused pins of the EXT MGMT Ethernet port. Connect a local management PC using the included RJ-45 to DB-9 adapter (please refer to the appendix). This RS-232 serial connection provides access to the iMcV-FiberLinX-II module configuration screens. These configuration screens are also accessible from a Telnet connection.

DHCP Disable (Static IP Addressing)

DHCP is disabled in the default configuration. Initially, modules are assigned a Static default IP Address of 10.10.10.10. Changes to the Static IP Address can be added manually through iConfig, an RS-232 Serial session, or Telnet. The changes will be initiated following reboot of the module.

DHCP Enable (Dynamic IP Addressing)

If a DHCP server is present on the network and DHCP is enabled, the DHCP client will initiate a dialogue with the server during the boot up sequence. The server will then issue an IP address to the management card. Once the new IP address is received, the SNMP Management Module will reboot so that the new IP address will take effect. Refer to About Serial Port Configuration for more information about Enabling/Disabling DHCP.

When there is no DHCP server on the network, use iConfig or serial configuration to manually set the IP addresses.

When DHCP is enabled, the IP address (default 10.10.10.10 or user configured) is saved. When DHCP is disabled, the saved IP address will be reinstated and the device will reboot.

DHCP servers give out lease times: devices renew their leases based on the administrator-specified time. If a device cannot renew its lease, and the lease expires, the device will be given the IP address 10.10.10.10 and will reboot.

iView² Management Software

iView² is the IMC Networks management software designed specifically for the IMC Networks iMcV family of modules. It features a Graphical User Interface (GUI) and gives network managers the ability to monitor and control the manageable IMC Networks products.

iView² is available in several versions and can also function as a snap-in module for HP OpenView Network Node Manager. For assistance in selecting the right version of iView² for a specific operating system, please visit:
http://www.imcnetworks.com/products/iview2.cfm

iView² supports the following platforms:

- Windows 98
- Windows NT
- Windows 2000
- Windows XP
- Windows Vista

In addition, there are Java versions of iView² for other Java capable operating systems such as Linux.

iConfig Utility

iConfig is a configuration utility in iView² that allows the user to quickly and easily complete the initial SNMP configuration for IMC Networks' SNMP-manageable devices. iConfig can set the IP address, set the Subnet Mask and Default Gateway, define the Community Strings, and define SNMP Traps. iConfig can also be used to upload new versions of unit software.

iConfig offers an authorized IP address system and access restriction to MIB groups supported by the IMC Networks manageable devices. These extra layers of security are purely optional and do not effect SNMP compatibility in any way.

Default Username/Password

The default user ID and password for both iConfig and Telnet are the following:

User: admin / Password: admin

For information on how to set/change passwords, see *Password Protection/Changing Password*.

NOTE
It is the responsibility of the network administrator to store and maintain the password lists.

Installation

Each iMcV-FiberLinX-II module requires one slot in an iMediaChassis or MediaChassis. To install the module in a chassis, remove the blank faceplates covering the slots where the module is to be installed. Then slide the module into the chassis card guides until the module is seated securely in the connector. Secure the module to the chassis by tightening the captive screw.

The iMcV-FiberLinX-II module includes on-board SNMP logic. A chassis other than an iMediaChassis series cannot manage an iMcV-FiberLinX-II, so the iMcV-FiberLinX-II must be managed independently.

When installed in an iMediaChassis, the iMcV-FiberLinX-II module can be managed from the chassis by using the Unified Management Agent (UMA). Refer to http://www.imcnetworks.com/Products/Unified_Management_Agent.cfm for more information on using UMA with iConfig, iMediaChassis and iMcV-FiberLinX-II. iMcV-FiberLinX-II modules not managed by UMA must have an IP address assigned to them after installation before they can be managed. Refer to *(I) - Assigning IP Information* for more information.

Small Form-Factor Pluggable Ports (SFP)

iMcV-FiberLinX-II modules are available with an optional SFP port. Since the SFP port speed is fixed at 100Mbps, it is necessary to use a 100 Mbps speed SFP. In addition, many SFPs, including those from IMC Networks, feature enhanced diagnostics capabilities with a Digital Diagnostics Monitoring Interface (DDMI). DDMI statistics provide real-time access to transceiver operating parameters such as voltage, temperature, laser bias current, and both transmitted and received optical power. DDMI information can be accessed in iView^2 by clicking **Tables** > **SFP Info**.

NOTE
iMcV-FiberLinX-II has been tested with the IMC Networks SFP modules, so it is possible to install any MSA-compliant SFP module. However, IMC Networks does not guarantee the functionality of non-IMC Networks SFP modules due to possible non-conformity with MSA design standards.

AutoCross Feature for Twisted Pair Connection

All twisted pair ports on the iMcV-FiberLinX-II include AutoCross, a feature that automatically selects between a crossover workstation and a straight-through connection depending on the connected device.

LED Operation

iMcV-FiberLinX-II features diagnostic LEDs as shown below.

TX/FX LEDs

FDX/COL:
- Glows yellow when port is operating in Full-Duplex.
- Blinks yellow when collisions occur on port.

LNK/ACT:
- Glows green when link is established on port.
- Blinks green during data activity on port.

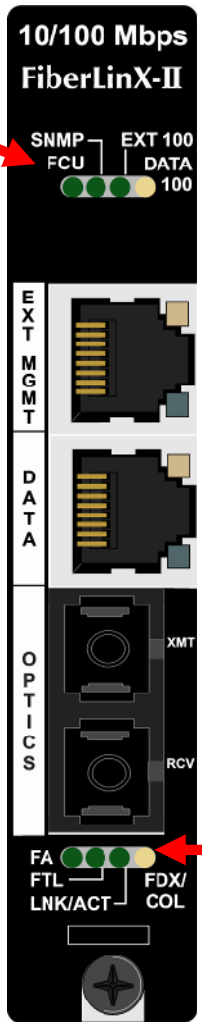
Diagnostic LEDs

FCU (Far CPU Up):
- Host: Glows green when far end is detected.
- Remote: Glows green when unit is configured as Remote.
- Standalone Unit: LED remains OFF.

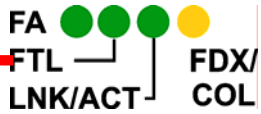
SNMP:
This LED glows green to indicate that this is an SNMP manageable module.

EXT 100:
Glows green when EXT MGMT port is operating at 100 Mbps.

DATA 100:
Glows yellow when DATA port is operating at 100 Mbps.



Optics Port LEDs



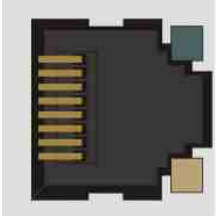
FA:
Glows green when FiberAlert is enabled.

FTL (Far TX Link):
- Host: Glows green when a link is established on remote (far-end) DATA port.
- Remote: Glows green when unit is configured as Remote.
- Standalone: LED remains OFF.

LNK/ACT (Link/Activity):
- Glows green when link is established on port.
- Blinks green during data activity on port.

FDX/COL (Full Duplex/Collision):
- Glows yellow when port is operating in Full-Duplex.
- Blinks yellow when collisions occur on port.

TX/SFP LEDs



LNK/ACT:

- Glows green when link is established on port.
- Blinks green during data activity on port.

FDX:

- Glows yellow when port is operating in Full-Duplex.
- Blinks yellow when collisions occur on port.

Diagnostic LEDs

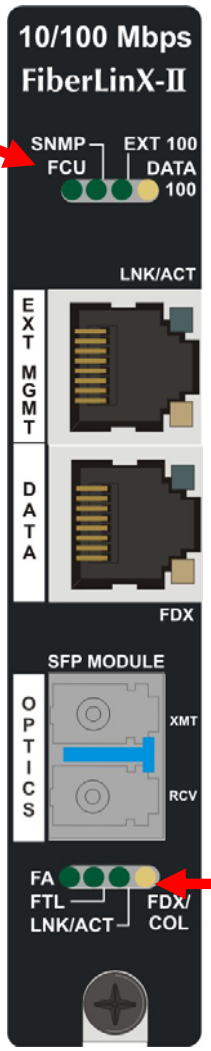
FCU (Far CPU Up):

- Host: Glows green when far end is detected.
- Remote: Glows green when unit is configured as Remote.
- Standalone Unit: LED remains OFF.

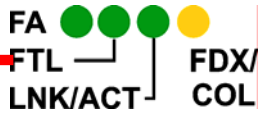
SNMP:
This LED glows green to indicate that this is an SNMP manageable module.

EXT 100:
Glows green when EXT MGMT port is operating at 100 Mbps.

DATA 100:
Glows yellow when DATA port is operating at 100 Mbps.



Optics Port LEDs



FA:
Glows green when FiberAlert is enabled.

FTL:

- Host: Glows green when a link is established on remote (far-end) DATA port.
- Remote: Glows green when unit is configured as Remote.
- Standalone: LED remains OFF.

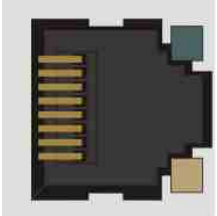
LNK/ACT (Link/Activity):

- Glows green when link is established on port.
- Blinks green during data activity on port.

FDX/COL (Full Duplex/Collision):

- Glows yellow when port is operating in Full-Duplex.
- Blinks yellow when collisions occur on port.

SFP/SFP LEDs



LNK/ACT:

- Glows green when link is established on port.
- Blinks green during data activity on port.

FDX:

- Glows yellow when port is operating in Full-Duplex.
- Blinks yellow when collisions occur on port.

Diagnostic LEDs

FCU (Far CPU Up):

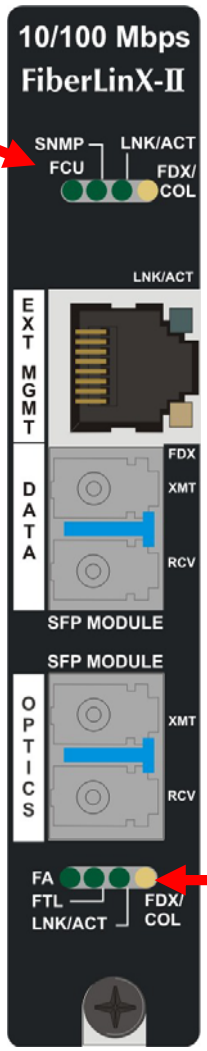
- Host: Glows green when far end is detected.
- Remote: Glows green when unit is configured as Remote.
- Standalone Unit: LED remains OFF.

SNMP:
This LED glows green to indicate that this is an SNMP manageable module.

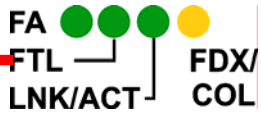
LNK/ACT (Link/Activity):

- Glows green when link is established on port.
- Blinks green during data activity on port.

DATA 100:
Glows yellow when DATA port is operating at 100 Mbps.



Optics Port LEDs



FA:
Glows green when FiberAlert is enabled.

FTL:

- Host: Glows green when a link is established on remote (far-end) DATA port.
- Remote: Glows green when unit is configured as Remote.
- Standalone: LED remains OFF.

LNK/ACT (Link/Activity):

- Glows green when link is established on port.
- Blinks green during data activity on port.

FDX/COL (Full Duplex/Collision):

- Glows yellow when port is operating in Full-Duplex.
- Blinks yellow when collisions occur on port.

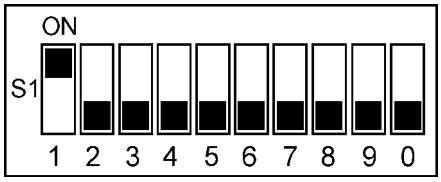
Hardware Configuration

Before installing the module in a chassis, there are two features that must be selected using DIP Switches. These selections include the following:

- Enable/Disable management on each port (DIP Switches 1, 2, and 3).
- Configure the module to be either a standalone, a host, or a remote (DIP Switches 7 and 8).

DIP Switch Settings

Before installing the iMcV-FiberLinX-II, use the DIP Switches to set the hardware-configurable features. The DIP Switches are located on switch S1 on the iMcV-FiberLinX-II card. Refer to the diagram and table for switch settings and available features.



Switch	Function	Default Setting
1	*Management on EXT MGMT port*	*ON*
2	*Management on DATA port*	*OFF*
3	*Management on OPTICS or UPLINK port*	*OFF*
4	***Factory use - Do not change***	*OFF*
5	***Factory use - Do not change***	*OFF*
6	***Factory use - Do not change***	*OFF*
7	*Remote Module*	*OFF*
8	*Host Module*	*OFF*
9	***Factory use - Do not change***	*OFF*
0	***Factory use - Do not change***	*OFF*

Host/Remote and Standalone Units

The iMcV-FiberLinX-II can be used as a Host, Remote, or Standalone unit. Refer to the *Application Examples* section for examples.

When two iMcV-FiberLinX-II units are used as a pair, configure one as a Host unit (DIP Switch 8 = On) and the other as a Remote unit (DIP Switch 7 = On). As a host unit, the iMcV-FiberLinX-II requests management information from the attached remote unit. It then displays that information, along with its own, when queried by SNMP. As a Remote unit, the iMcV-FiberLinX-II will respond to requests for management information from an attached Host unit.

The iMcV-FiberLinX-II default configuration is as a Standalone unit (DIP Switches 7 and 8 = Off).

Management

Although the iMcV-FiberLinX-II provides a twisted pair port solely for management (EXT MGMT), the iMcV-FiberLinX-II can be configured to accept IP-based management traffic from any of its three ports. Enable management on more than one port, or disable management on all of the ports, as desired. These switches limit only IP-based management. Host-to- Remote management is IP-less and is never blocked from the fiber port. Serial port management of the unit is always available on the EXT MGMT port regardless of the DIP Switch settings.

In addition to defining which ports are used to manage the iMcV-FiberLinX-II units, the management DIP Switch settings also define what ports the flow of the Network Provider's Management Domain traffic can take through the unit. See *Application Examples* for information regarding the Management Domain.

DIP Switch 1 = On for management on the EXT MGMT port.
DIP Switch 2 = On for management on the DATA port.
DIP Switch 3 = On for management on the OPTICS or UPLINK port.

Software Configuration

The following sections describe the features that can be configured. Refer to the iView² online help for iMcV-FiberLinX-II module configuration information.

Assigning IP Information

When the iMcV-FiberLinX-II is installed in an iMediaChassis, use UMA to manage the iMcV-FiberLinX-II without an IP address (refer to the iView² online help for more information on UMA). When the iMcV-FiberLinX-II is not installed in an iMediaChassis, SNMP-management is not accessible until the iMcV-FiberLinX-II IP information (e.g., IP address, subnet mask, etc.) is configured (using iConfig, a serial port craft connection, or DHCP). After assigning iMcV-FiberLinX-II an IP address, use iView² or another SNMP-compatible Network Management System (NMS) to remotely configure, monitor and manage the iMcV-FiberLinX-II.

Auto Negotiation, Duplex Mode, and Speed

The DATA and EXT MGMT ports on the iMcV-FiberLinX-II module Auto Negotiate for speed and duplex mode. This module also provides the option of selectively advertising or forcing the speed and duplex mode.

Auto Negotiation

The iMcV-FiberLinX-II ships from the factory with Auto Negotiation enabled on the twisted-pair ports. In this mode, the ports negotiate for speed and duplex.

Forcing the Speed and Duplex Mode

Manually set the twisted-pair ports on the iMcV-FiberLinX-II for 10 Mbps or 100 Mbps operation at Half- or Full-Duplex (i.e., 10 Mbps Full-Duplex, 10 Mbps Half-Duplex, 100 Mbps Full-Duplex, etc.). The Optics Port operates at 100Mbps Full-Duplex.

Selective Advertising

Selective Advertising, when used in combination with Auto Negotiation, advertises only the configured speed and duplex mode for the twisted pair port. If a specific speed and/or duplex mode are desired, IMC Networks recommends using Selective Advertising, rather than Force Mode, when connecting to devices that only use Auto Negotiation.

Bandwidth Control

The iMcV-FiberLinX-II includes bi-directional bandwidth control in 32 Kbps increments (configurable via iView²). This allows the bandwidth limit to be set independently from the DATA Port to the OPTICS (or UPLINK) Port and vice versa in a single iMcV-FiberLinX-II application. In a dual iMcV-FiberLinX-II application, it can

be set from the Host unit to the Remote unit and vice versa (i.e., the bandwidth on the DATA ports on both the Host and Remote modules can be limited independently).

NOTE
Management packets do not have priority over data packets.

Configuration File Save/Restore Function

Requirements

FiberLinX-II family series:

Minimum firmware version required: A4
iMcV-FiberLinX-II: A1 or higher,
Required iView² version: 1.8.4 or higher

The Configuration File Save/Restore Function allows a user the ability to backup all the configuration settings of a unit. With this backup, a user can restore settings to a unit if necessary or use this backup to apply the same settings to a different unit.

All configurable managed objects are saved in a configuration file that is stored in the unit's Large File Area. This includes all configurable settings such as VLAN configurations, IP Address configuration and SNMP agent settings. The configuration file can be transferred from the unit to a PC and saved to disk through the iConfig protocol. The configuration file can be transferred from a PC to a unit of the same type through iConfig or TFTP into the unit's Large File Area. After the transfer is complete, the unit copies the configuration to flash and reboots.

The configuration file's contents is device-type specific and can be identified by iConfig as a configuration file as well as to what type of device it is applicable to.

How to Save a Configuration File

To save a configuration file, use the iConfig tool. Log into the unit through iConfig, navigate to the iConfig Administration tab, select the "S**ave Configuration**" button, wherein a prompt requires a file name, as well as any user notes. From this point the file will be transferred to the PC's disk through the iConfig network protocol.

Once the file is saved to disk it can be restored to the device or sent to another like device through iConfig or TFTP.

For iConfig The user will log into a unit, select the Administration tab, select the **Upload Configuration** button, be prompted to locate a configuration file on the PC's disk. From this point the file transfer will take place from the PC to the unit. After a successful transfer, the user will be prompted to Reboot to make the new configuration active.

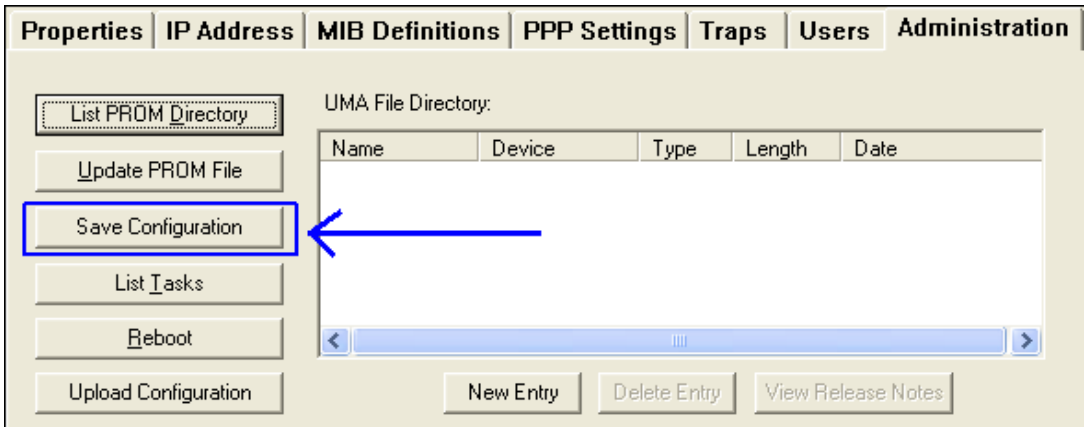
For TFTP The user will log into the unit either through a serial port session or through Telnet. They will navigate to the download command page, enter the TFTP server's IP address and enter the configuration file name, then press **Enter** to start the download process. Once the download is successful, the user will be prompted to apply the settings. The device must be rebooted after applying the settings to make them active.

By default, the IP Address configuration currently on the device is kept intact and not overwritten by the new configuration file.

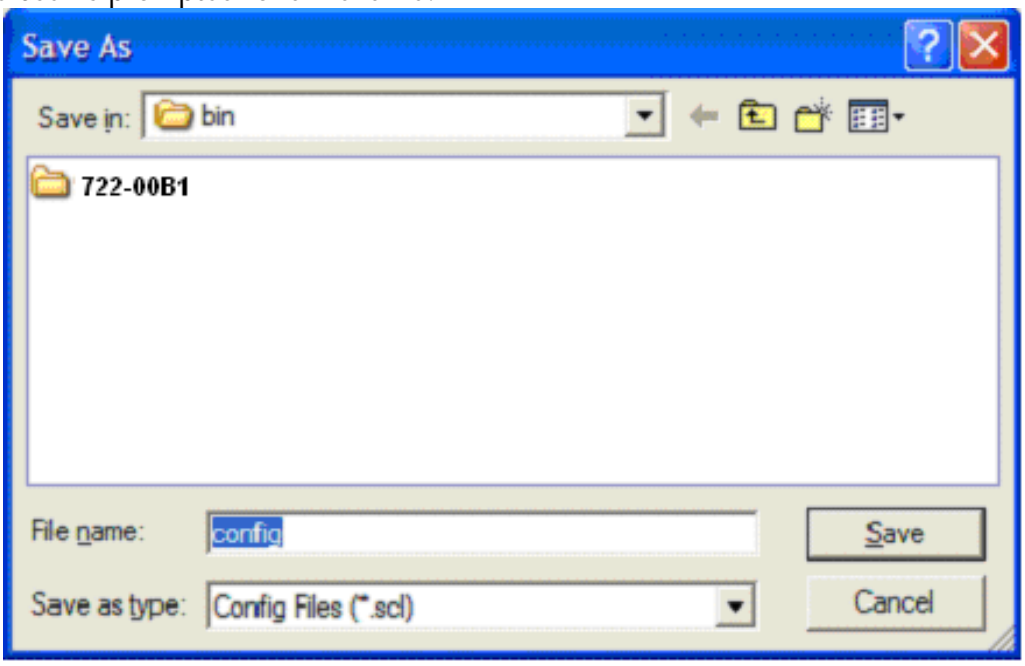
Configuration File Basics

Saving a Configuration File to Disk:

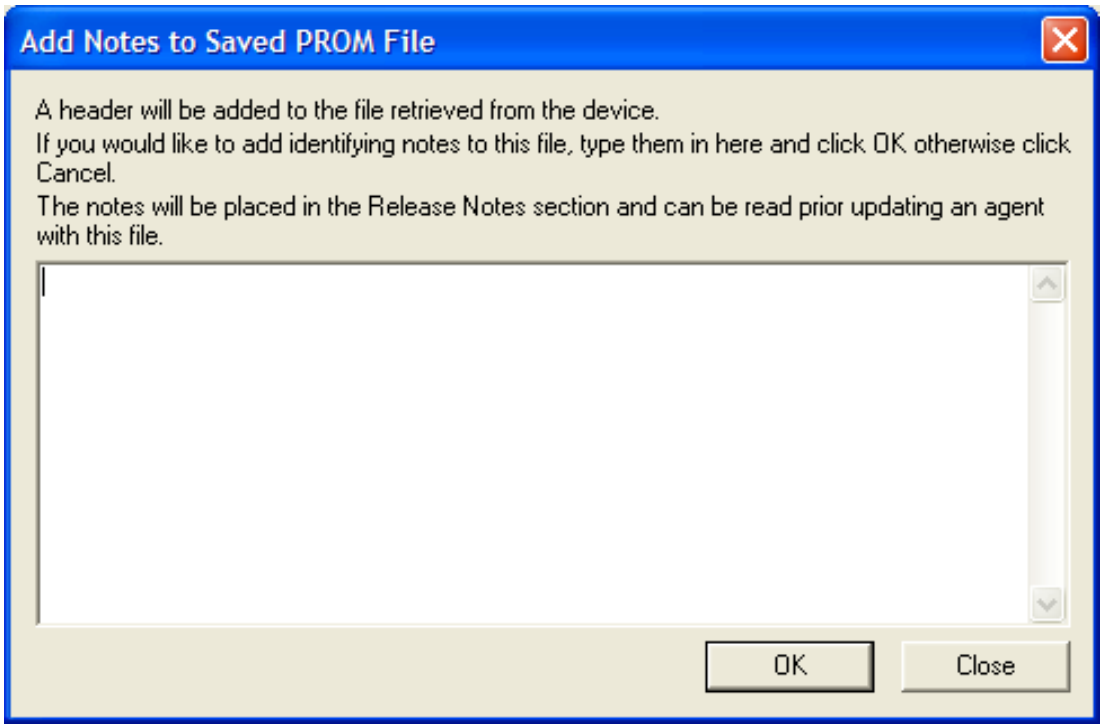
From the Administration Tab in iConfig click the **Save Configuration** button:



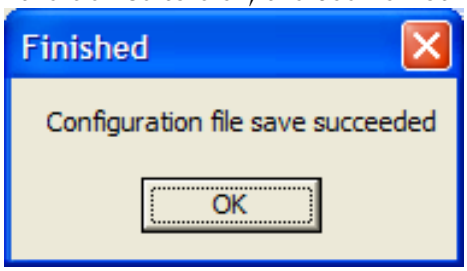
The user is prompted for a filename:



The user is prompted to enter any notes to the header of the saved file for future reference when uploading the file through iConfig:

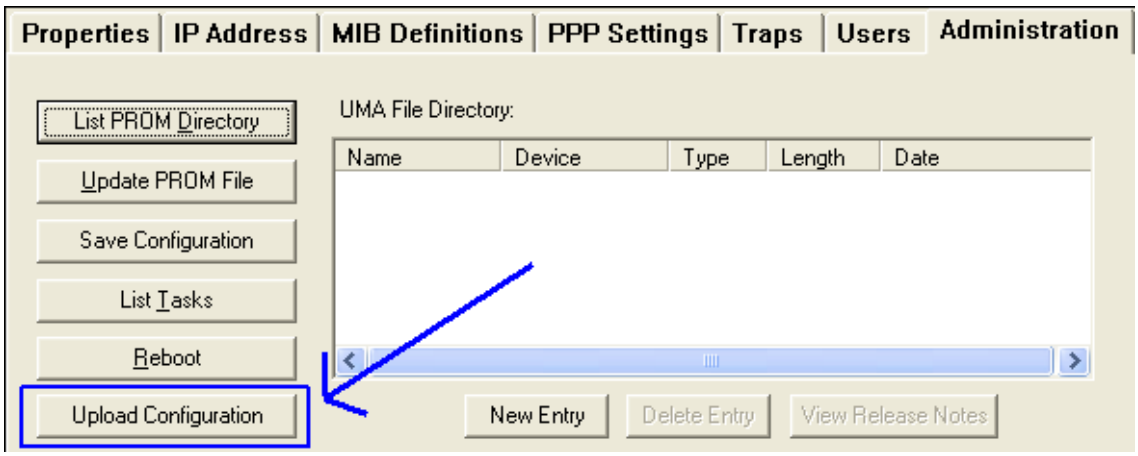

Add Notes to Saved PROM File
A header will be added to the file retrieved from the device.
If you would like to add identifying notes to this file, type them in here and click OK otherwise click Cancel.
The notes will be placed in the Release Notes section and can be read prior updating an agent with this file.
OK
Close

After the file transfer from the device to disk, the user is notified of the status:

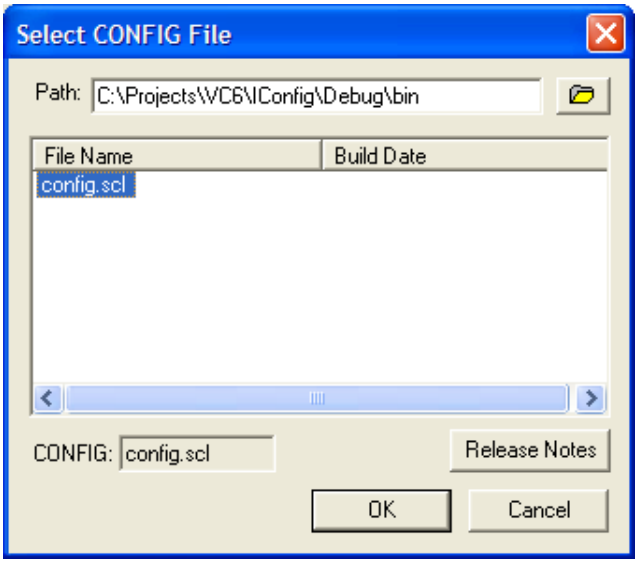


Uploading a Saved Configuration File through iConfig

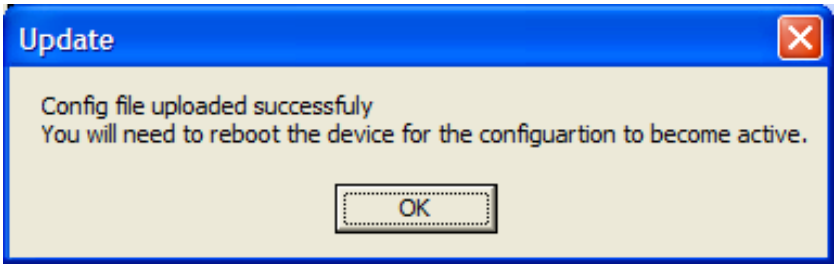
From the Administration Tab in iConfig click the **Upload Configuration** button:



The user will be prompted to select a configuration file. Once selected, the user can also view any notes that were added when the file was saved:



After selecting the configuration file, the file upload process begins; when completed, the user is notified of the status and also notified that a reboot is necessary for the new configuration to become active:

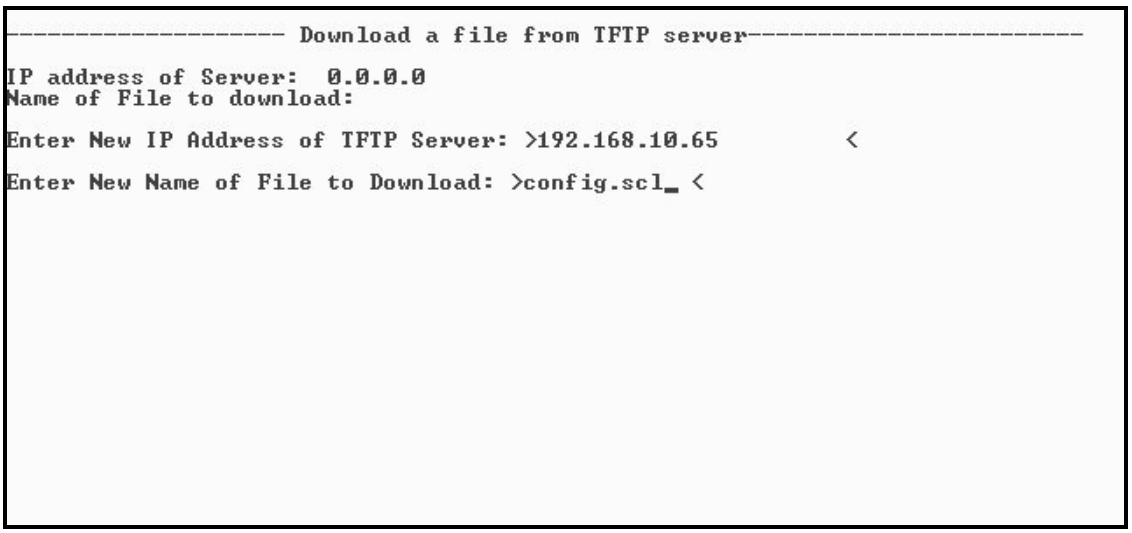


Uploading a Saved Configuration File through TFTP

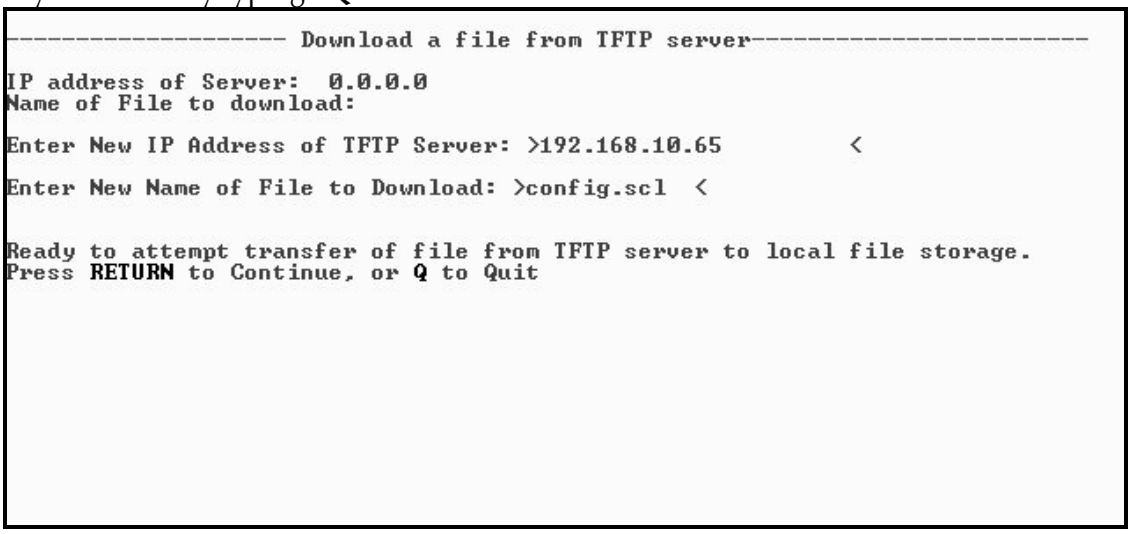
From the commands list in the CLI (Serial or Telnet) run the download command by typing in **download**:

```
Command         Description
--------        -----------
cleandb         Reboot With Clean Database
download        File Download from TFTP Server
ifstats         Display Port Statistics
rmstats         Display Port RMON Statistics
version         Show Firmware Version
reboot          Reboot Unit
security        Configure Non-Standard Network Settings
port            Display And Change Port Settings
config          Set mode of operation
accounts        Add or Delete Username/Password Accounts
sysdescr        Change System Descriptions
unit            Display And Change Unit Settings
bw              Display And Change Bandwidth Settings
sfpstats        Display SFP DDMI Info



->download
Press RETURN To Go Back To Main Screen.
```

In the download command screen type in the IP Address of the TFTP server and the file name to retrieve.



The user will be prompted to continue that retrieval process by pressing the **ENTER** key or cancel by typing "**Q**".



After the transfer process is complete the user will be prompted to press the **Enter** key again to load the configuration file:

```
-------------------- Download a file from TFTP server------------------------

IP address of Server:  0.0.0.0
Name of File to download:

Enter New IP Address of TFTP Server: >192.168.10.65         <

Enter New Name of File to Download: >config.scl  <


Ready to attempt transfer of file from TFTP server to local file storage.
Press RETURN to Continue, or Q to Quit
Transfer Block Counter: 143
An SNMP Configuration file has been downloaded from the TFTP
Server and has been put in local storage.

Press RETURN to load the configuration data from this
file into the device's SNMP configuration area.
Press Q to  Not LOAD the configuration data,
but leave the file in local storage.
-
```

Once loaded into the device's SNMP memory area, the user will be prompted to **reboot** the device to make the new configuration active:

FX/TX LinkLoss and FiberAlert

During normal operation, link integrity pulses are transmitted by all point-to-point Ethernet devices. When an iMcV-FiberLinX-II receives valid link pulses, it knows that the device to which it is connected is up, and that the copper or fiber cable coming from that device is intact. The appropriate LNK (link) LED is lit to indicate this. For troubleshooting information utilizing the LinkLoss and FiberAlert features of the iMcV-FiberLinX-II modules, refer to *Troubleshooting* at the end of this manual.

**** WARNING ****

FiberAlert and LinkLoss features cause data interruptions designed to alert remote sites of line failures. These data interruptions can be misinterpreted as module failures when these features are enabled. Enable these features only when the resulting data interruptions and causes are well understood.

FX LinkLoss

FX LinkLoss is a link integrity monitoring feature that forwards fiber link faults to the RJ-45 Data port to indicate that a fiber link fault has occurred.

TX LinkLoss

TX LinkLoss is a link integrity monitoring feature that forwards an RJ-45 link fault to the fiber connected device to indicate that a link fault has occurred.

FiberAlert

FiberAlert minimizes the problems associated with the loss of one strand of fiber. Normally when a single strand of fiber is lost, the transmitting side of the connection

is unaware that there is a fault. FiberAlert returns faults back on the fiber they came in on.

Using LinkLoss and FiberAlert

In a typical central site to remote site media conversion, it is recommended that the enable the LinkLoss and FiberAlert features are enabled as indicated in the following:

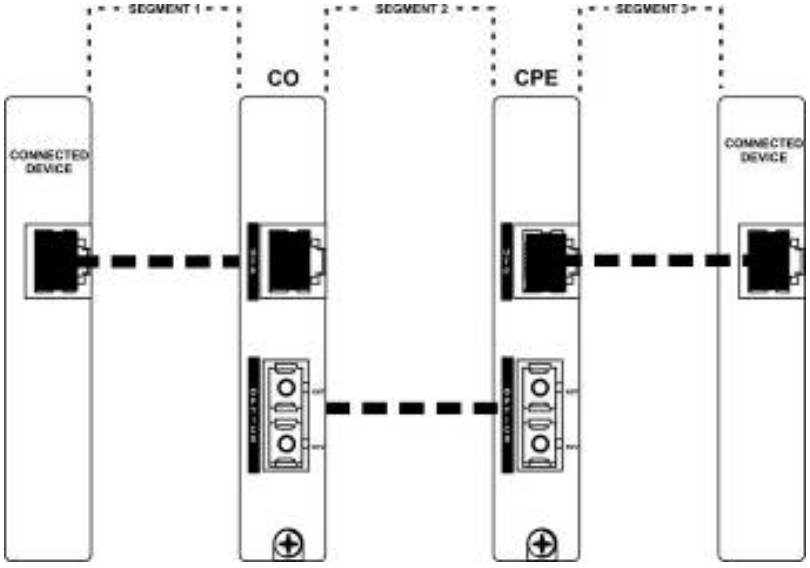
FiberAlert and LinkLoss			
Feature	**Enabled**	**Fault Location**	**Port affected**
FiberAlert	Remote Side Only	Fiber	Fiber
TX LinkLoss	Remote Side (or both)	Twisted Pair	Fiber
FX LinkLoss	Host Side (or both)	Fiber	Twisted Pair

** WARNING **
Do not enable FiberAlert on both modules when using iMcV-FiberLinX-II in pairs. This will cause them to lock up when a fault occurs on the fiber. Only enable FiberAlert on the remote module.

Link Fault Pass Through (LFPT)

Link Fault Pass Through is a troubleshooting feature that combines TX and FX LinkLoss from both the local and remote modules. LFPT is enabled by turning on both FX and TX LinkLoss on both modules. This feature allows either end of the conversion to detect a link fault occurring at the other end of the media conversion chain.

Regardless whether a break occurs on a copper or fiber segment between the End device and the media converter, or between the two media converters, End devices at both ends.



Regardless if there is a break in segment 1, 2 or 3, the link will drop on the switches at both ends.

The link fault is passed through the media conversion and is observed at each end. It acts just like it would if the devices were directly connected.

NOTE
FiberAlert can also be added to the remote side of the pair to further assist in locating a fault.

Last Gasp

The iMcV-FiberLinX-II includes a Last Gasp feature, which sends a trap Flinx Unit Down for the Host unit or a Flinx Remote Unit Down for the Remote unit (as seen in iView2) when the power to the module fails.

Loopback Testing

The following functions are available during loopback testing. During loopback testing, management traffic entering the uplink port is still capable of managing the device. This is selectable form the UNIT screen in a serial/Telnet session. There are no LoopBack test options in iView2

The menu of choices in the CLI includes:

- No loopback, normal traffic mode
- Loopback Enabled
- Loopback, Source/Destination address swap
- Loopback, address swap and clear Multicast bit

Loopback Testing on Remote or Standalone

Source/Destination Address Swap

A Layer 2 Ethernet switch will discard all received packets with the same MAC address as sent packets. To avoid this issue the Loopback feature can swap the source and destination MAC addresses on the looped data. (This selection can cause a frame with a multicast source address to be created, which violates the IEEE standard.)

Address Swap and Clear Multicast Bit

In addition to swapping the source and destination MAC addresses on the looped data, the Loopback feature can also be set to clear the multicast bit. This allows the looped data to avoid being blocked by any multicast settings.

Loopback Testing in a Host/Remote Configuration

Configure the Host by selecting No Learning on OPTICS and DATA Ports; on the Remote, choose SRC/DST Address Swap or Address Swap and Clear Multicast Bit.

No Learning on OPTICS and DATA Ports

The Loopback feature can be set to disable address learning on the OPTICS (or UPLINK) and DATA ports, allowing the loopback to be performed without interference from MAC address filtering functions. This is a function on the HOST unit. Set the REMOTE unit for Loopback then set the HOST to disable learning so Loopback frames pass from the Optics port to the Data port.

Remote:Source/Destination Address Swap

A Layer 2 Ethernet switch will discard all received packets with the same MAC address as sent packets. To avoid this issue the Loopback feature can swap the source and destination MAC addresses on the looped data.

OR

Address Swap and Clear Multicast Bit

In addition to swapping the source and destination MAC addresses on the looped data, the Loopback feature can also be set to clear the multicast bit. This allows the looped data to avoid being blocked by any multicast settings.

NOTE
Units should not be in the Default Mode when performing LoopBack tests.

Broadcast Storm Protection

Broadcast Storm Protection allows setting the maximum broadcast packet rate allowed as a percentage of line speed (from 0% - 20%). The suggested value is 1%.

Using Telnet

It is necessary to assign the iMcV-FiberLinX-II an IP address before using a Telnet session (this is not necessary when using UMA). Refer to the *Assigning IP Information* section for more information. All of the configurations that can be performed from the serial port can also be performed using a Telnet session; only one Telnet session can be launched at a time.

The following are the three levels for Telnet account access:

User: View status, change own password, and reboot.

Operator: All User privileges mentioned above, plus ability to change settings.

Administrator: Operator privileges mentioned above, plus ability to add/delete accounts and reinitialize the unit to default settings (cleandb).

Serial Configuration/Telnet Session

The following sections describe serial configuration (including VLAN configuration), Telnet session configuration, and DHCP configuration.

NOTE
Some screens may show TX and FX for the port titles where TX = DATA port and FX = OPTICS (or UPLINK) port. The examples are from firmware version 512-00A2.

Serial Port (EXT MGMT)

NOTE
The serial port (EXT MGMT) is always set to Administrator level. The password for Telnet sessions is the password that is set and used in iConfig (refer to the iConfig section for more information).

After running through an initial self test, the screen will display the following message: Press <Enter> for Device Configuration. Press **Enter** open the main configuration screen:

```
Saved Values. <These values will be active after reboot>
    IP Address      -  10.10.10.10
    Subnet Mask     - 255.0.0.0             DHCP is not active
    Default Gateway - 000.000.000.000
    Server IP Addr  - 000.000.000.000
    New Prom File   - filename

Current Values. <These values are in use now>
    IP Address      -  10.10.10.10
    Subnet Mask     - 255.0.0.0
    Default Gateway - 000.000.000.000
    Server IP Addr  - 000.000.000.000
    New Prom File   - filename

Community String: public     Access: r/w

Press I to enter new saved parameter values. Press P to change Password.
Press T to enter new Trap Destination. Press K to remove ALL Trap Destinations.
Press C to enter new Community String. Press U to remove ALL Community Strings.
Press E to End session. Type REBOOT to reboot unit. Press D for DHCP On/Off.
Press SpaceBar for additional commands.
```

This screen contains the following information and options:

Saved and Current Values

Saved values display the changes made during the current session and current values display the values currently in use:

- IP Address (IP address of SNMP agent)
- Subnet Mask (mask to define IP subnet to which agent is connected)
- Default Gateway (default router for IP traffic outside of the subnet)
- Server IP Address (TFTP server)
- New Prom File (TFTP new file name)

Command List

I = Enter new **Saved Parameter Values**
P = Change the **Password***
T = Enter new **Trap Destinations**
K = Remove **All Trap Destinations**
C = Create **SNMP Community Strings**
U = Delete All **SNMP Community Strings**
E = **End** the session*
Reboot = Reboot the unit (may result in short data loss)
D = Enable or disable **DHCP**
Space Bar = Opens the device specific configuration options screen.

* Individuals with User-level rights can only view port status and port settings, change their password, end a session, and reboot the unit.

NOTE
*It is necessary to reboot the iMcV-FiberLinX-II after making any modifications to the Saved Values for the changes to take effect. To reboot, type **Reboot** at the prompt on the Main Configuration screen.*

Assigning IP Information

To modify the Saved Parameter Values (i.e., assign the IP address and subnet mask), press **I**. The system prompts for the IP address and subnet mask for the connected device. Press **Enter** after each entry. A default gateway can be assigned to allow the unit to be visible beyond the local network (press **Enter** to skip). When finished, press **Enter**, then type **Reboot** for the changes to take effect. The Current Values on the Main Configuration screen are updated to match the Saved Values.

Password Protection/Changing Password

Passwords have the following requirements:

- The password must be between 1 and 8 characters long
- The password consists of a combination of any ASCII characters except spaces
- Passwords are case sensitive

Password protection is provided for the serial configuration process by pressing **P** on the main configuration screen. Enter a password, keeping in mind that passwords are case-sensitive and must not exceed eight characters or include spaces, and press **Enter**. This password will be requested whenever logging on. To remove password protection, select **P** and, instead of entering a password, press **Enter**.

Passwords are a way to make the management of the IMC Networks devices secure, but these password lists must be stored and maintained. If a password is lost, neither users (including administrators) nor IMC Networks have a way to decode it. Refer to the iView^2 iConfig online help for more password information.

If the serial password is forgotten, it is necessary to contact tech support for assistance in resetting the password. If the iConfig username and password are forgotten, launch a console session through the serial port, and type in the command **cleandb**. If both the serial and the iConfig passwords are forgotten, please contact technical support at 1-800-624-1070.

Assigning SNMP Trap Destinations

Traps are sent by the manageable device to a management PC when a certain event takes place. To enter a trap destination, press **T**. When prompted, enter the IP address of the destination device and press Enter. Next, type the name of the community string (that the destination device has been configured to accept) and press **Enter**. Select whether the trap is for SNMP version 1 or 2c and press Enter. This function enables all of the device traps. Use iConfig to configure the device to selectively activate and de-activate traps.

Supported traps include: Link Down, Link Up, Cold Start, Warm Start, Last Gasp, and Authentication Failure.

When deployed in pairs, iMcV-FiberLinX-II also supports the following traps:

- Remote Unit Lost
- Remote Unit Found
- Far End TX Link Up
- Far End TX Link Down
- Remote Unit Cold Start
- Remote Unit Warm Start

Removing All SNMP Trap Destinations

To remove all trap destinations, press **K**. Press **Y** to continue when prompted and remove all trap destinations, or press **N** to abort. Press **Enter** to finish.

This function will delete all trap destinations. To selectively delete trap destinations or select the type of trap reported or not reported, use iConfig to configure the device.

Creating SNMP Community Strings

The default community string is named public and has read/write access. It is recommended that custom community strings are created (with read-only access for general use and another with read/write access for the administrator) and tested before deleting Public. To create a new community string, go to the main configuration screen and press **C**. Enter the name of the new community (up to 16 characters, no spaces) and press **Enter**. Then type one of the following to assign the community string's access rights:

- R = read-only access
- W = read/write access
- Enter = abort

Deleting All SNMP Community Strings

To delete all community strings and start over, press **U**. Press **Y** when prompted to proceed and delete all community strings, **N** to abort. Press **Enter** to finish.

This function will delete all community strings. To selectively delete community strings, use iConfig to configure the device.

Ending The Session

Press **E** to end the session before disconnecting the serial cable. This will stop the continuous stream of data that is sent to the serial port.

Reboot Device

By typing **Reboot**, the device will restart, which will result in a temporary loss of operation of the unit while it re-initializes.

Enabling DHCP

By pressing **D**, a screen will appear which allows enabling or disabling DHCP for the device. By default, the DHCP client is disabled.

Commands List (Space Bar)

The iMcV-FiberLinX-II also includes several device-specific options. To access these options, press the **Space Bar** from the Main Configuration screen, type the name of the action to be performed (as shown below) and press **Enter**.

```
Command         Description
--------        -----------
cleandb         Reboot With Clean Database
download        File Download
ifstats         Display Port Statistics
rmstats         Display Port RMON Statistics
version         Show Firmware Version
reboot          Reboot Unit
security        Configure Non-Standard Network Settings
port            Display And Change Port Settings
config          Set mode of operation
accounts        Add or Delete Username/Password Accounts
sysdescr        Change System Descriptions
unit            Display And Change Unit Settings
bw              Display And Change Bandwidth Settings

->
Press RETURN To Go Back To Main Screen.
```

Command	Description
cleandb	Allows reboot of the unit with a clean database.
download	Downloads firmware from Server IP address using TFTP.
ifstats	Displays interface statistics.
rmstats	Displays RMON statistics.
version	Displays the firmware and hardware version information.
reboot	Reboots the unit.
security	Allows non-standard network configuration.
port	Display/configure port status values.
config	Configure VLAN and Transparent modes of operation.
accounts	Add/delete Username/Password accounts.
sysdescr	Enter the MIB-II system description information.
unit	Display and change unit settings.
bw	Display and change bandwidth settings.

Clean Database—cleandb

There are two levels of cleandb: The first level resets the Telnet/iConfig password and all of the SNMP database values. The second level additionally resets the IP address, IP Subnet, Gateway, VLAN settings, CLI command settings, serial port password and security settings.

Downloading Files—download

The iMcV-FiberLinX-II allows downloading firmware from a central server by using TFTP. To download firmware by using either a serial connection or a Telnet session, perform the following:

1. In the Main Configuration screen, enter the TFTP server IP Address and the name of the Prom file to be downloaded (case sensitive).
2. Reboot the unit to make these settings current.
3. Press the **Space Bar** from the Command List section in the Main Configuration screen. The Device-Specific Options screen displays.
4. Type **download** and press **Enter**. The Download a File screen displays with the IP Address of the TFTP server and the name of the file to download. Confirm that the server IP address and the filename are correct.
5. Press **Enter**. The release notes are displayed. Use the **Space Bar** to page through the notes.
6. After reviewing the notes, enter **Y** to start downloading the file.
7. The download progress displays and ends with a successful download message or with an error message.
8. Press **Q** or **F4** to return to the Device-Specific Options screen.

When the iMcV-FiberLinX-II is installed in a managed chassis, it is possible to use UMA to update the firmware (refer to the iView^2 online help for more information on using UMA with iConfig, iMediaChassis and iMcV-FiberLinX-II).

Port Configuration—port

The iMcV-FiberLinX-II allows viewing port status and configuring some port features from a serial connection or a Telnet session. In the Commands list, type **port** and press **Enter** to access the Port Status/Control screen.

In the Port Status Values area of this screen it is possible to view the link status, link lost counter, duplex status, and port speed.

```
------------------------   Port Status Values   ----------------------------
                  Optics                Data                 EXT Mgmt

Link Status       Up                    Up                   Down
Link Lost Cntr    0                     0                    0
Duplex Status     Full                  Full                 Half
Port Speed        100 Mbits             100 Mbits            10 Mbits

------------------------  Port Control Settings  --------------------------
                                        Data                 EXT Mgmt

Port Enable                             Enabled              Enabled
Admin Status                            Up                   Up
Port Speed Ctrl                         Autoneg.             Autoneg.
Advertise Ctrl                          Advert All           Advert All
Advertise FlowC                         Adv Flow             Adv Flow
Force FlowCtrl    Frc FlowCt            Flow Auto            Flow Auto
Unit FlowControl  Ena. FlowC

Use Arrow Keys To Move Cursor. Press Space Bar To Change Value.
Press RETURN To Set New Value. Press Q Or F4 To Exit
```

In the Port Control Settings area of the Port screen it is possible to set the following:

Port Enable - Enable or disable the port. Both Port Enable and Admin Status must be enabled (enabled and up) to enable the port. This setting can be disabled from iView^2.

Admin Status - Enable (Up) or disable (Down) the port. Both Port Enable and Admin Status must be enabled (enabled and up) to enable the port. This setting can be disabled from MIB-II compatible software.

Port Speed Ctrl - Set the port for Auto Negotiation or to force one of the following speeds:

- 10 Mbps Half-Duplex
- 10 Mbps Full-Duplex
- 100 Mbps Half-Duplex
- 100 Mbps Full-Duplex.

Advertise Ctrl - This is the Selective Advertising feature. Selective Advertising is used in combination with Auto Negotiation to advertise the selected speed and duplex mode for the DATA and EXT MGMT ports. This allows advertising: all speeds and duplex modes; 10 Mbps Half-Duplex; 10 Mbps Full-Duplex; 100 Mbps Half-Duplex; 100 Mbps Full-Duplex; 10 Mbps Half and Full-Duplex; etc. Auto Negotiation must be enabled for Selective Advertising to work.

NOTE
If a specific speed and/or duplex mode are desired, IMC Networks recommends using Selective Advertising, instead of Force Mode, when connecting to devices that can only Auto Negotiate. For the FO uplink versions, the port is always force flow control 100 FDX and cannot be changed.

Advertise FlowC and Force FlowCtrl—the following are Advertise Control features.

When using Flow Control functionality on any port, enable Flow Control (refer to *Unit Flow Control* for more information). Next, configure each port individually:

- To use Auto Negotiation and Flow Control:
  Advertise FlowC = Advertise Flow, Force FlowCtrl = Flow Auto
- To use Auto Negotiation but not Flow Control
  Advertise FlowC = No Flow
- To use Flow Control and force the port speed (Port Speed Ctrl)
  Advertise FlowC = Advertise Flow, Force FlowCtrl = Frc FlowCt

All RJ-45 ports feature Flow Control in Full-Duplex and Back Pressure Flow control in Half-Duplex. Back Pressure Flow Control is a hardware based flow control that forces collisions on the line to limit bandwidth.

Unit FlowControl - Enable or disable Flow Control functionality on the unit. This must be enabled to use Flow Control on any port.

Mode Configuration—config

The iMcV-FiberLinX-II can be configured to allow several combinations of VLAN tagging and management. This manual refers to the most useful combinations as modes. The applications of these modes are described in detail in the *Application Examples* section.

- Mode One – Default and Default Plus
- Mode Two – Transparency with Untagged Management
- Mode Three - Transparency with Tagged Management
- Mode Four - Transparency with Extra Tagging (Q-in-Q)
- Mode Five - Port VLAN
- Mode Six – Port VLAN Filter

NOTE
Default mode is the factory default and is provided as a starting point from which to configure the iMcV-FiberLinX-II modules. This mode does not provide adequate management isolation and is not recommended for normal use.

This section describes the Telnet/serial port screens and fields available for configuring the iMcV-FiberLinX-II modes.

The iMcV-FiberLinX-II modes are configured using the **config** command from the Device-Specific Options screen. This opens the Transparent Mode screen or the VLAN Mode screen depending on the current configuration.

Transparent Mode

The Transparent Mode screen is displayed when the iMcV-FiberLinX-II module is configured in Default mode or Transparent mode.

```
Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches
set to on, all traffic passes between Optics and Data port EXCEPT what has
been defined as the Management Domain. The Management Domain can either be
defined as untagged traffic or traffic with a specified VLAN ID.

In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off,
all traffic passes between the Optics and Data Ports.

Default Mode – the unit passes only Untagged Packets.

The unit is currently in Default Mode.

Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to
move to other options [ Y ]
```

Transparent Mode Setup Screen

When Transparent Mode is enabled, the next screen is the Transparent Mode Setup screen:

```
                    TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [ N ]

Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ N ]

Are VLAN Tags required on the EXT Port?       [ N ]

Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes

Reboot is required for any change to take affect.
```

The following parameters can be set in this screen:

- VLAN Tag on Management Packets
- Extra Tag Mode
- VLAN Tag on EXT MGMT port

Transparent Mode Setup

This parameter makes it possible to use all untagged data as the management domain by entering **N**, or to define a VLAN ID tag for the management domain by entering **Y**. When **Y** is entered, this field expands to display the Management Tag field and the Management Priority field.

```
                    TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [ Y ]
       The Management Tag is  [7   ]
       Management Priority is [0   ]

Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ N ]

Are VLAN Tags required on the EXT Port?       [ N ]

Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes

Reboot is required for any change to take affect.
```

*****WARNING*****

If the device is currently managed on any port other than the EXT MGMT port, do not leave the Management Tag field defined as zero (0). This will disable management traffic on the iMcV-FiberLinX-II. It is necessary to enter a VLAN ID between 1 and 4094 (excluding the VLAN ID used for the Extra Tag).

Transparent with Extra-Tagging

This parameter allows adding a VLAN ID tag to all traffic (tagged or untagged) arriving on the DATA port by entering **Y**. This ID can optionally be kept or removed when leaving the DATA port. When **Y** is entered, this field expands to display the Data Tag, Data Priority, Leave Tags on Data Port, and TPID fields. The TPID setting allows setting the EtherType of the Extra Tag frame to either 8100 (standard), 9100 (special use), or 9200 (special use).

```
                    TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [ N ]

Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ Y ]
       The Data Tag is         [20  ]
       Data Priority is        [7   ]
Are Extra Tags left on the Data Port?          [ N ]

Select the TPID for the Extra Tag   1 = 8100, 2 = 9100, 3 = 9200
       Extra Tag TPID [ 1 ]   [8100]

Are VLAN Tags required on the EXT Port?        [ N ]

Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes

Reboot is required for any change to take affect.
```

Transparent with VLAN Tag on EXT MGMT Port

This parameter adds the management VLAN ID tag to all untagged data arriving at the EXT MGMT port by entering **N**, or can restrict the EXT MGMT port to only accept data tagged with the management VLAN ID by entering **Y**.

```
                  TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [ Y ]
       The Management Tag is  [7   ]
       Management Priority is [0   ]

Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ N ]

Are VLAN Tags required on the EXT Port?       [ N ]

Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes

Reboot is required for any change to take affect.
```

VLAN Mode Screen

When **N** is entered in the Transparent Mode Setup screen, the VLAN Mode screen displays:

```
Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.

           VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
Ports                                          Data VLANs are used only
Optics  [0   ]   [0   ]    [0  ]    [0  ]   [ N ]  if Tags are enabled on both
Data    [0   ]   [0   ]    [0  ]    [0  ]   [ N ]  the Optics and Data Ports.
Management VLAN                              EXT Mgmt Tag
SNMP    [0   ]   [0   ]    [0  ]    [0  ]   [ N ]

Data Vlans  <Optics <----> Data>
VLAN  1 [0   ]   [0   ]  VLAN 12 [0   ]   [0   ]   VLAN 23 [0   ]   [0   ]
VLAN  2 [0   ]   [0   ]  VLAN 13 [0   ]   [0   ]   VLAN 24 [0   ]   [0   ]
VLAN  3 [0   ]   [0   ]  VLAN 14 [0   ]   [0   ]   VLAN 25 [0   ]   [0   ]
VLAN  4 [0   ]   [0   ]  VLAN 15 [0   ]   [0   ]   VLAN 26 [0   ]   [0   ]
VLAN  5 [0   ]   [0   ]  VLAN 16 [0   ]   [0   ]   VLAN 27 [0   ]   [0   ]
VLAN  6 [0   ]   [0   ]  VLAN 17 [0   ]   [0   ]   VLAN 28 [0   ]   [0   ]
VLAN  7 [0   ]   [0   ]  VLAN 18 [0   ]   [0   ]   VLAN 29 [0   ]   [0   ]
VLAN  8 [0   ]   [0   ]  VLAN 19 [0   ]   [0   ]   VLAN 30 [0   ]   [0   ]
VLAN  9 [0   ]   [0   ]  VLAN 20 [0   ]   [0   ]   VLAN 31 [0   ]   [0   ]
VLAN 10 [0   ]   [0   ]  VLAN 21 [0   ]   [0   ]   VLAN 32 [0   ]   [0   ]
VLAN 11 [0   ]   [0   ]  VLAN 22 [0   ]   [0   ]
Valid Vlan IDs are between 1 and 4094. Valid priorities are between 0 and 7.
Type S or F3 to save the changes. Type Q or F4 to quit and cancel changes.
```

The following parameters can be set in this screen:

- Default Mode
- Port VLAN on OPTICS (or UPLINK) port
- Port VLAN on DATA port
- Management VLAN
- Port VLAN Filter

Default Mode

Entering **N** in the Tags column of both the Optics and Data rows will place the iMcV-FiberLinX-II in Default mode.

```
Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.

          VLAN IDs          Priorities      Tags
       Current   Saved    Current   Saved
 Ports                                          Data VLANs are used only
 Optics  [0   ]   [0   ]    [0  ]    [0  ]    [ N ] if Tags are enabled on both
 Data    [0   ]   [0   ]    [0  ]    [0  ]    [ N ] the Optics and Data Ports.
 Management VLAN                          EXT Mgmt Tag
 SNMP    [0   ]   [0   ]    [0  ]    [0  ]    [ N ]
```

No VLANs are defined allowing only untagged packets to pass through the unit.

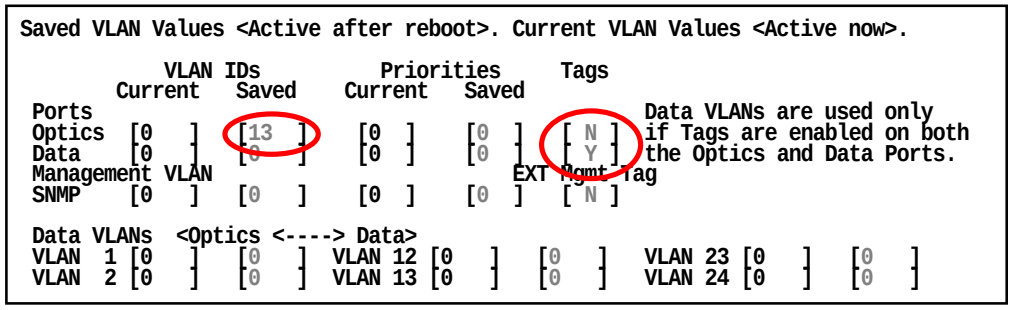
Port VLAN on OPTICS (or UPLINK) port

This parameter restricts traffic to a single VLAN ID tag for the OPTICS (or UPLINK) port by entering **Y** in the Tags column of the Optics row and **N** in the Tags column of the Data row. In the VLAN IDs - Saved column of the Data row, enter the VLAN ID tag to be used (in this example, 13). This VLAN ID will be added to all untagged traffic entering the DATA port and removed from all traffic leaving the DATA port.

```
Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.

          VLAN IDs          Priorities      Tags
       Current   Saved    Current   Saved
 Ports                                          Data VLANs are used only
 Optics  [0   ]   [0   ]    [0  ]    [0  ]    [ Y ] if Tags are enabled on both
 Data    [0   ]   [13  ]    [0  ]    [0  ]    [ N ] the Optics and Data Ports.
 Management VLAN                          EXT Mgmt Tag
 SNMP    [0   ]   [0   ]    [0  ]    [0  ]    [ N ]

 Data VLANs  <Optics <----> Data>
 VLAN  1 [0   ]   [0   ]  VLAN 12 [0   ]   [0   ]   VLAN 23 [0   ]   [0   ]
 VLAN  2 [0   ]   [0   ]  VLAN 13 [0   ]   [0   ]   VLAN 24 [0   ]   [0   ]
 VLAN  3 [0   ]   [0   ]  VLAN 14 [0   ]   [0   ]   VLAN 25 [0   ]   [0   ]
 VLAN  4 [0   ]   [0   ]  VLAN 15 [0   ]   [0   ]   VLAN 26 [0   ]   [0   ]
 VLAN  5 [0   ]   [0   ]  VLAN 16 [0   ]   [0   ]   VLAN 27 [0   ]   [0   ]
 VLAN  6 [0   ]   [0   ]  VLAN 17 [0   ]   [0   ]   VLAN 28 [0   ]   [0   ]
 VLAN  7 [0   ]   [0   ]  VLAN 18 [0   ]   [0   ]   VLAN 29 [0   ]   [0   ]
 VLAN  8 [0   ]   [0   ]  VLAN 19 [0   ]   [0   ]   VLAN 30 [0   ]   [0   ]
 VLAN  9 [0   ]   [0   ]  VLAN 20 [0   ]   [0   ]   VLAN 31 [0   ]   [0   ]
 VLAN 10 [0   ]   [0   ]  VLAN 21 [0   ]   [0   ]   VLAN 32 [0   ]   [0   ]
 VLAN 11 [0   ]   [0   ]  VLAN 22 [0   ]   [0   ]
Valid VLAN IDs are between 1 and 4094. Valid priorities are between 0 and 7.
Type S or F3 to save the changes. Type Q or F4 to quit and cancel changes.
```

Port VLAN on DATA Port

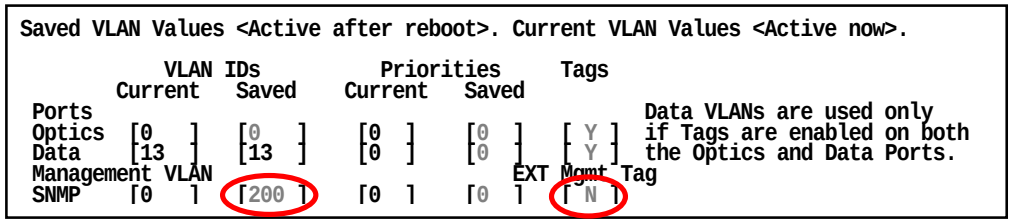
This parameter restricts traffic to a single VLAN ID tag for the DATA port by entering **Y** in the Tags column of the Data row and **N** in the Tags column of the Optics row. In the VLAN IDs - Saved column of the Optics row, enter the VLAN ID tag to be used (in this example, 13). This VLAN ID will be added to all untagged traffic entering the OPTICS (or UPLINK) port and removed from all traffic leaving the OPTICS (or UPLINK) port.



Management VLAN and EXT MGMT Tag

This parameter configures a VLAN ID for management traffic by entering an ID in the VLAN IDs – Saved column of the SNMP row (in this example, 200).

The EXT MGMT tag parameter provides the option of adding the defined Management VLAN ID to all untagged traffic entering the EXT MGMT port (EXT Mgmt Tag = N) or restricting the EXT MGMT port to pass only traffic bearing this VLAN ID (EXT Mgmt Tag = Y)

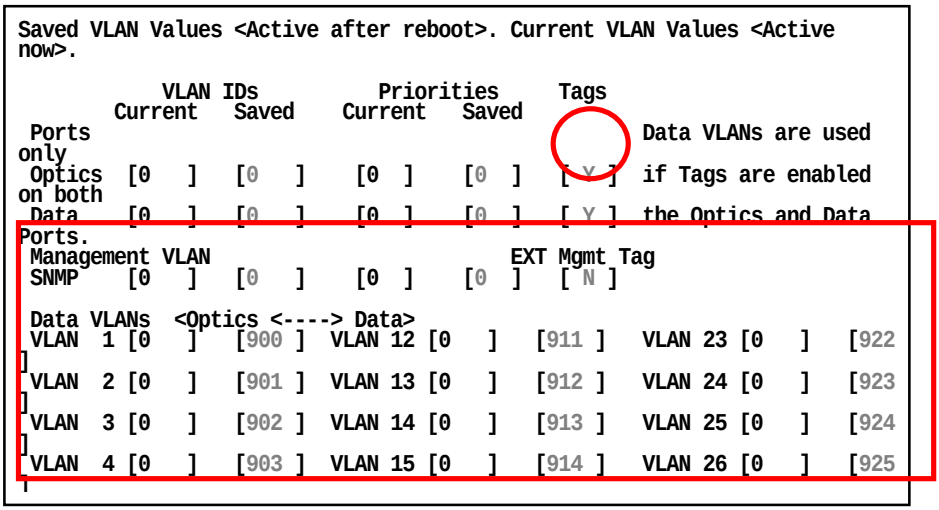


*****WARNING*****

If the device is currently managed on any port other than the EXT MGMT port, do not leave the Management Tag field defined as zero (0). This will disable management traffic on the iMcV-FiberLinX-II. It is necessary to enter a VLAN ID between 1 and 4094 (excluding the VLAN IDs used for the Port VLAN or for the Data VLANs).

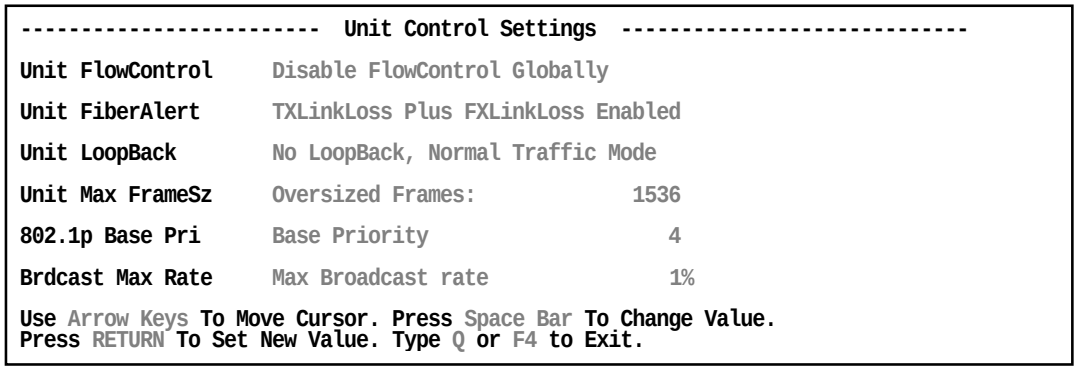
Port VLAN Filter

This parameter allows passing traffic with up to 32 separate VLAN IDs between the OPTICS (or UPLINK) port and the DATA port. To enable the Data VLANS fields, enter **Y** in the Tags column for both the Optics and Data rows. Enter up to 32 VLAN IDs in the Data VLANs fields; VLAN IDs can be any number between 1 and 4,094.


Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.
VLAN IDs
Current Saved
Priorities
Current Saved
Tags
Ports only
Optics [0] [0] [0] [0] [Y]
Data [0] [0] [0] [0] [Y]
Data VLANs are used if Tags are enabled on both the Optics and Data Ports.
Management VLAN
SNMP [0] [0] [0] [0]
EXT Mgmt Tag
[N]
Data VLANs <Optics <----> Data>
VLAN 1 [0] [900] VLAN 12 [0] [911] VLAN 23 [0] [922
VLAN 2 [0] [901] VLAN 13 [0] [912] VLAN 24 [0] [923
VLAN 3 [0] [902] VLAN 14 [0] [913] VLAN 25 [0] [924
VLAN 4 [0] [903] VLAN 15 [0] [914] VLAN 26 [0] [925

Unit Configuration—unit

The iMcV-FiberLinX-II allows viewing unit status as well as configure some unit features by using a serial connection or a Telnet session. In the Main Configuration screen, press the **Space Bar**, type **unit**, and press **Enter** to open the Unit Control Settings screen. In this screen it is possible to view the unit FlowControl, FiberAlert/LinkLoss, Loopback, Maximum Frame Size, and 802.1p Base Priority (logging-in as a User in a Telnet session allows viewing these settings, but prevents changing the settings).


Unit Control Settings
Unit FlowControl Disable FlowControl Globally
Unit FiberAlert TXLinkLoss Plus FXLinkLoss Enabled
Unit LoopBack No LoopBack, Normal Traffic Mode
Unit Max FrameSz Oversized Frames: 1536
802.1p Base Pri Base Priority 4
Brdcast Max Rate Max Broadcast rate 1%
Use Arrow Keys To Move Cursor. Press Space Bar To Change Value.
Press RETURN To Set New Value. Type Q or F4 to Exit.

Unit FlowControl – This enables/disables Flow Control functionality on the unit, and must be enabled to use Flow Control on any port. The settings include the following:

- Disable FlowControl Globally
- Enable FlowControl If Port Allows

Unit FiberAlert – Enables/disables FiberAlert and LinkLoss functionality on the unit. The settings include:

- No FiberAlert Or LinkLoss Enabled
- FXLinkLoss Only, Enabled
- TXLinkLoss Only, Enabled
- FiberAlert Plus FXLinkLoss Enabled
- FiberAlert Plus TXLinkLoss Enabled
- TXLinkLoss Plus FXLinkLoss Enabled
- TXLinkLoss + FXLinkLoss + FiberAlert Enabled
- FiberAlert Only

NOTE
FiberAlert is not offered on the all-copper (RJ-45) version of the iMcV-FiberLinX-II.

Unit LoopBack – Enables/disables Loopback functionality on the unit. The settings include the following:

- No LoopBack, Normal Traffic Mode
- LoopBack Enabled
- LoopBack, Src/Dest Address Swap
- LoopBack, Address Swap, Clear Multicast bit
- No Learning on OPTICS (or UPLINK) or DATA Ports

Unit Max FrameSz – Enter the maximum frame size on the unit by using the number keys.

- No VLAN–1518
- VLAN Tag–1522
- Oversized frames–1536
- Oversized frames–1916

802.1p Base Pri – Set the threshold between low and high priority on the unit. For example, when the Base VLAN Priority is set to 4, priority settings of 0 through 3 are low priority and settings of 4 through 7 are high priority. When the Base VLAN Priority is set to 3, priority settings of 0 through 2 are low priority and priority settings of 3 through 7 are high priority.

BrdCast Max Rate – Set the Broadcast Storm protection. Valid values are 0-20% where 0% disables Broadcast Storm protection. The setting is the percentage of line speed where broadcast frames will be dropped. For example, if the setting is 1% and the unit detects that broadcast traffic is exceeding 1% of the line speed then the unit will discard broadcast frames. The suggested setting is 1%.

Bandwidth Configuration—bw

The iMcV-FiberLinX-II allows viewing bandwidth status and configuring bandwidth from a serial connection or a Telnet session. In the Main Configuration screen, press the **Space Bar**, type **bw** and press **Enter** to access the Bandwidth Control Settings screen:

```
-----------------------  Bandwidth Control Settings  ----------------------------

                                      Optics Port     Data Port
RX Bandwidth Limit, 0 For None        0               0
TX Bandwidth Limit, 0 For None        0               0

Unit RateControl Enable/Disable       Disable

Use Arrow Keys To Move Cursor. Press Space Bar To Change Value.
Press RETURN To Set New Value. Press Q or F4 to Exit.
```

This screen includes the following parameters:

- Receive Bandwidth Limit
- Transmit Bandwidth Limit
- Unit Rate Control

RX Bandwidth Limit - Set the receive bandwidth limit (up to 100 Mbps) for both the DATA and OPTICS (or UPLINK) ports. Entering a setting of either 0 or 100,000,000 will result in a limit of 100 Mbps. When the received data reaches the set limit in a one second interval, the unit stops receiving data. If flow control is enabled, then flow control begins prior to reaching the set limit.

TX Bandwidth Limit – Set the transmit bandwidth limit (up to 100 Mbps) for both the DATA and OPTICS (or UPLINK) ports. Entering a setting of either 0 or 100,000,000 will result in a limit of 100 Mbps. When the transmit data reaches the set limit in a one second interval, the unit stops transmitting data, but will continue to receive until all the internal buffers are filled. If flow control is enabled, then flow control begins before all the buffers are filled.

NOTE
It is not recommended to set both the RX and TX Bandwidth limits at the same time. Setting TX Bandwidth Limits allows for full use of the memory buffers in the unit.

Unit RateControl Enable/Disable – Enable/disable the bandwidth limiting feature on this unit.

Application Overview

Before using iMcV-FiberLinX-II, decide the following:

- Will iMcV-FiberLinX-II units be located at only one or at both ends of the fiber?

- How will the iMcV-FiberLinX-II units be managed?
- Will VLAN IDs be defined?

How many iMcV-FiberLinX-II units will be used?

- Two for Host/Remote applications–allows IP-less management providing greater security
- One for a single unit application

How will the iMcV-FiberLinX-II be managed?

The iMcV-FiberLinX-II can be managed through any of its three ports (and any combination thereof) or from the chassis. Using the EXT MGMT/OPTICS (or UPLINK) port combination separates management traffic from the data and provides the highest level of security. UMA management does not require an IP address.

Will VLAN IDs be defined?

When VLAN traffic is used with specific tags on any/all of the DATA ports, it is necessary to disable Transparency and define VLAN IDs (refer to *VLAN Configuration* section). When it is desirable to use VLAN tagged, untagged, or double-tagged traffic, enable Transparency.

Application Examples

The following are application examples of the different VLAN configuration modes available using the iMcV-FiberLinX-II. If assistance is required to configure an application, contact IMC Networks Technical Support at techsupport@imcnetworks.com.

The application modes include the following:

- Mode One – Default and Default Plus
- Mode Two – Transparency with Untagged Management
- Mode Three - Transparency with Tagged Management
- Mode Four - Transparency with Extra Tagging (Q-in-Q)
- Mode Five - Port VLAN
- Mode Six - PortVLAN Filter

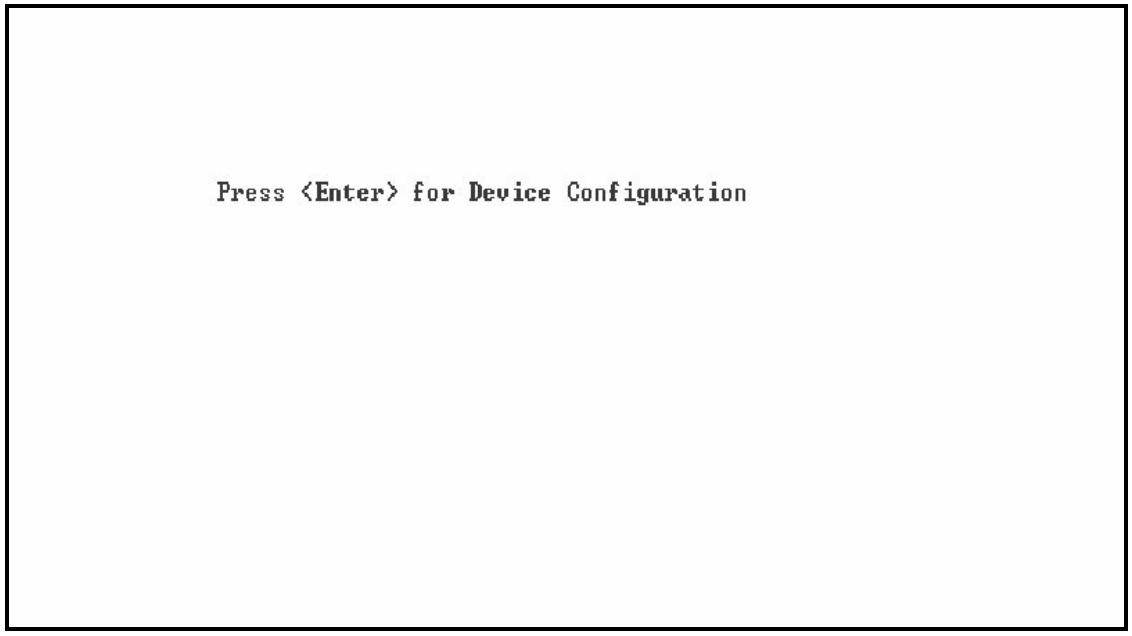
NOTE
When configuring VLAN IDs, remember to use any VLAN ID between 1 and 4,094. The VLAN IDs used in the following applications are for example purposes ONLY.

Mode One-Default and Default Plus Mode

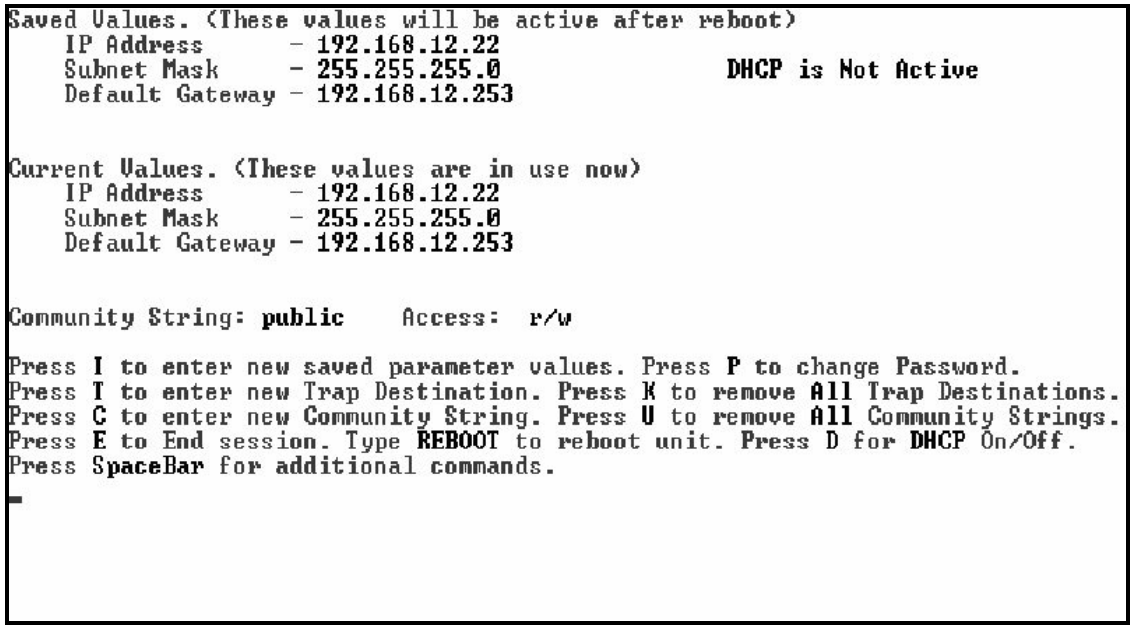
Default mode passes only untagged data between the DATA port and the OPTICS (or UPLINK) port. This mode is the factory default and is provided as a starting point

from which to configure the iMcV-FiberLinX-II modules. It is not intended as a mode for normal use. In Default Plus Mode, all tagged and untagged traffic passes between the Data and Optics ports. Management to the device must be untagged.

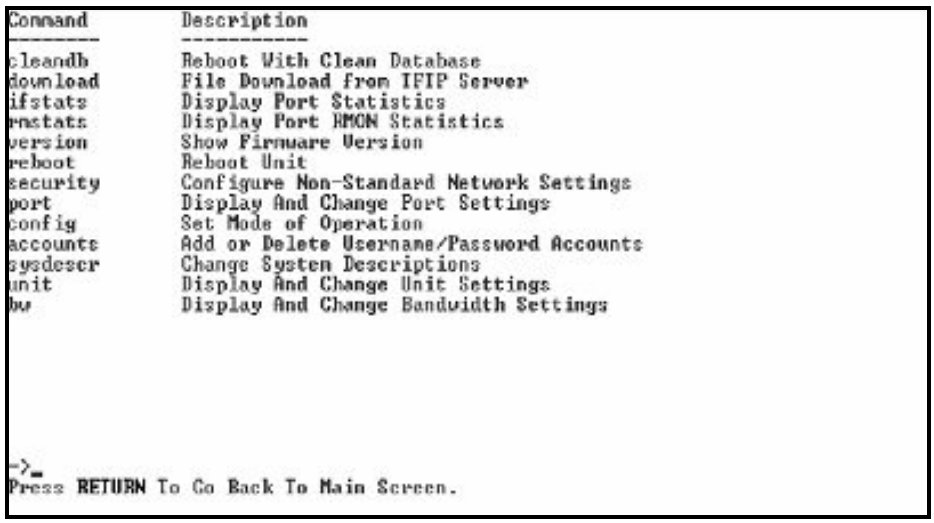
NOTE
Default Mode does not provide any management traffic protection and is not recommended for normal use.



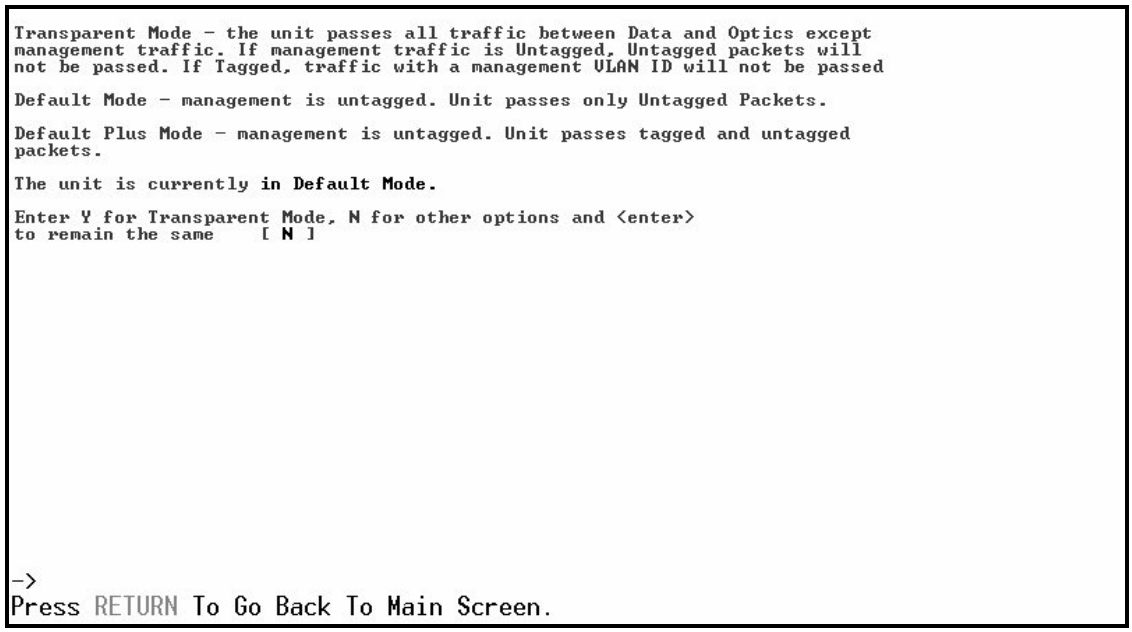
Press Enter for device configuration mode.


Saved Values. (These values will be active after reboot)
IP Address - 192.168.12.22
Subnet Mask - 255.255.255.0
DHCP is Not Active
Default Gateway - 192.168.12.253
Current Values. (These values are in use now)
IP Address - 192.168.12.22
Subnet Mask - 255.255.255.0
Default Gateway - 192.168.12.253
Community String: public Access: r/w
Press I to enter new saved parameter values. Press P to change Password.
Press I to enter new Trap Destination. Press K to remove All Trap Destinations.
Press C to enter new Community String. Press U to remove All Community Strings.
Press E to End session. Type REBOOT to reboot unit. Press D for DHCP On/Off.
Press SpaceBar for additional commands.

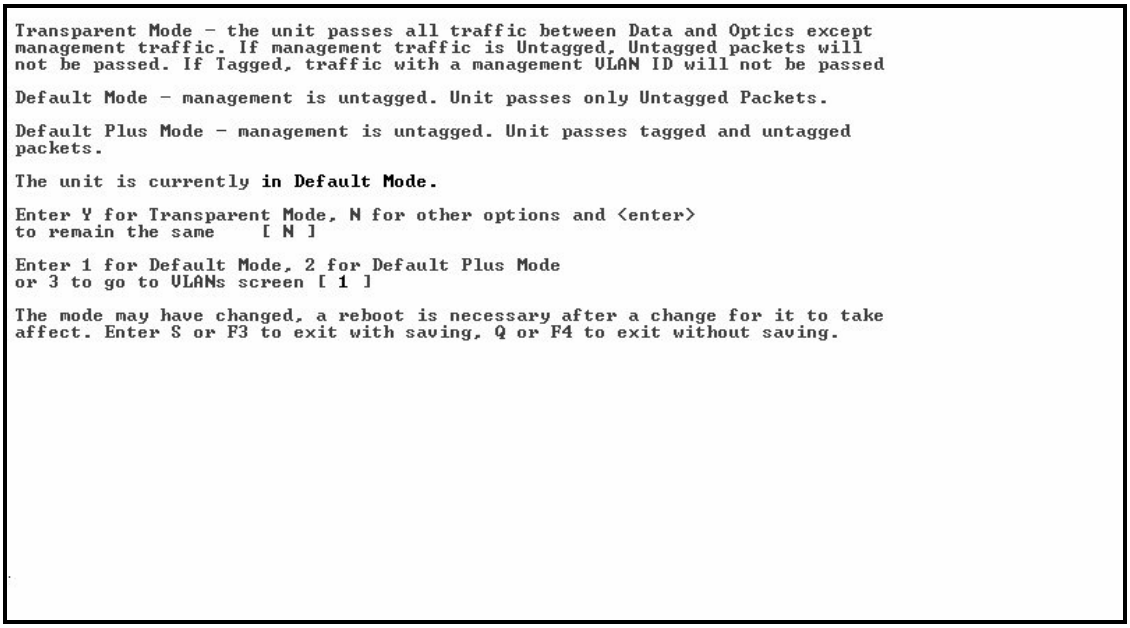
Press the Space Bar once to access additional commands.


Command Description
cleandb Reboot With Clean Database
download File Download from TFTP Server
ifstats Display Port Statistics
rmstats Display Port RMON Statistics
version Show Firmware Version
reboot Reboot Unit
security Configure Non-Standard Network Settings
port Display And Change Port Settings
config Set Mode of Operation
accounts Add or Delete Username/Password Accounts
sysdescr Change System Descriptions
unit Display And Change Unit Settings
bw Display And Change Bandwidth Settings
->
Press RETURN To Go Back To Main Screen.

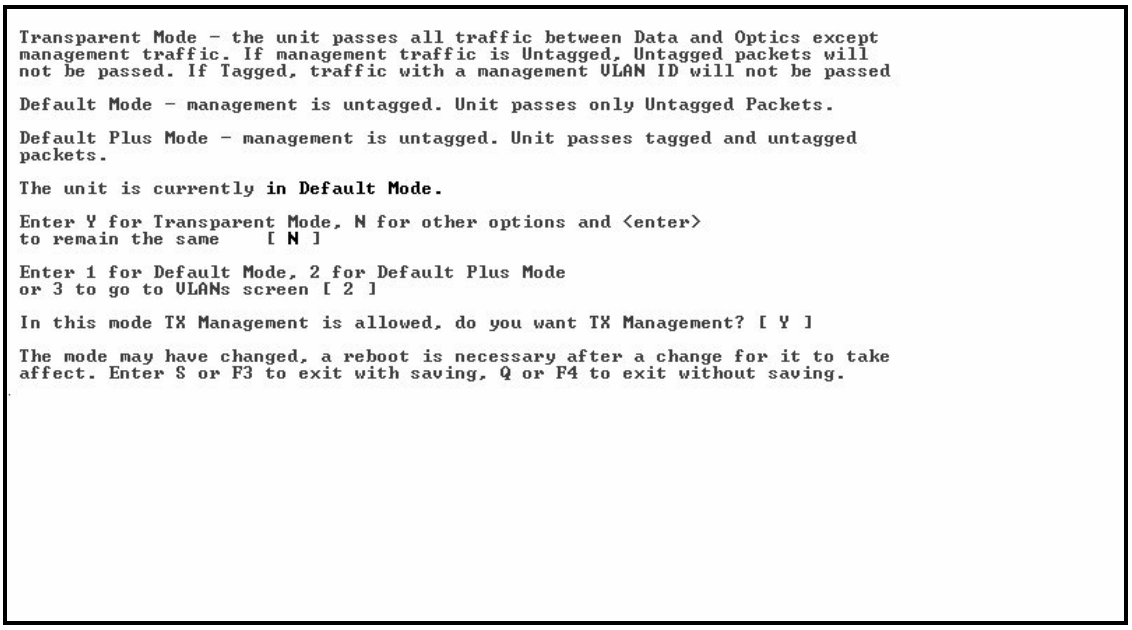
Type config then press **Enter** to set the operation mode.


Transparent Mode - the unit passes all traffic between Data and Optics except management traffic. If management traffic is Untagged, Untagged packets will not be passed. If Tagged, traffic with a management VLAN ID will not be passed
Default Mode - management is untagged. Unit passes only Untagged Packets.
Default Plus Mode - management is untagged. Unit passes tagged and untagged packets.
The unit is currently in Default Mode.
Enter Y for Transparent Mode, N for other options and <enter> to remain the same [N]
->
Press RETURN To Go Back To Main Screen.

Press **Enter** for other options.


Transparent Mode - the unit passes all traffic between Data and Optics except
management traffic. If management traffic is Untagged, Untagged packets will
not be passed. If Tagged, traffic with a management VLAN ID will not be passed
Default Mode - management is untagged. Unit passes only Untagged Packets.
Default Plus Mode - management is untagged. Unit passes tagged and untagged
packets.
The unit is currently in Default Mode.
Enter Y for Transparent Mode, N for other options and <enter>
to remain the same [N]
Enter 1 for Default Mode, 2 for Default Plus Mode
or 3 to go to VLANs screen [1]
The mode may have changed, a reboot is necessary after a change for it to take
affect. Enter S or F3 to exit with saving, Q or F4 to exit without saving.

Press **2** to change to Default Plus Mode, then press **Enter**.


Transparent Mode - the unit passes all traffic between Data and Optics except
management traffic. If management traffic is Untagged, Untagged packets will
not be passed. If Tagged, traffic with a management VLAN ID will not be passed
Default Mode - management is untagged. Unit passes only Untagged Packets.
Default Plus Mode - management is untagged. Unit passes tagged and untagged
packets.
The unit is currently in Default Mode.
Enter Y for Transparent Mode, N for other options and <enter>
to remain the same [N]
Enter 1 for Default Mode, 2 for Default Plus Mode
or 3 to go to VLANs screen [2]
In this mode TX Management is allowed, do you want TX Management? [Y]
The mode may have changed, a reboot is necessary after a change for it to take
affect. Enter S or F3 to exit with saving, Q or F4 to exit without saving.

Mode Two-Transparency with Untagged Management

Transparent with Untagged Management mode passes tagged traffic between the DATA port and the OPTICS (or UPLINK) port and isolates untagged traffic as management domain traffic (untagged).

To configure this mode, do the following:

1. Set the management DIP Switch ON for the ports using management (in this example it is the OPTICS (or UPLINK) port: 3 = ON). To enable External Management (EXT MGMT), set DIP Switch 1 to ON. (otherwise, leave DIP Switch 1 in the OFF position (default from factory) to disable EXT MGMT)

2. Set Transparent Mode to allow both tagged data and untagged management traffic to pass:

   a. In the Main Configuration screen, press the **Space Bar** and type **config**. The Configuration Screen displays:

```
Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches
set to on, all traffic passes between Optics and Data port EXCEPT what has
been defined as the Management Domain. The Management Domain can either be
defined as untagged traffic or traffic with a specified VLAN ID.

In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off,
all traffic passes between the Optics and Data Ports.

Default Mode – the unit passes only Untagged Packets.

The unit is currently in Default Mode.

Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to
move to other options [ Y ]
```

   b. Enter **Y** in the Transparent Mode field and press any key (except S or Q) to open the Transparent Mode Setup screen.

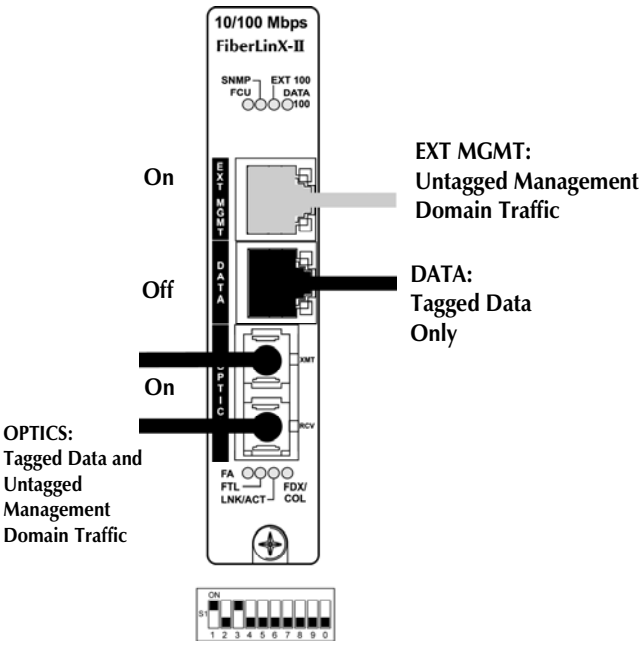
```
                    TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [ N ]

Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ N ]

Are VLAN Tags required on the EXT Port?       [ N ]

Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes

Reboot is required for any change to take affect.
```

   c. Press **S** or **F3** to save without setting any transparent mode options. This will set all untagged traffic as management.

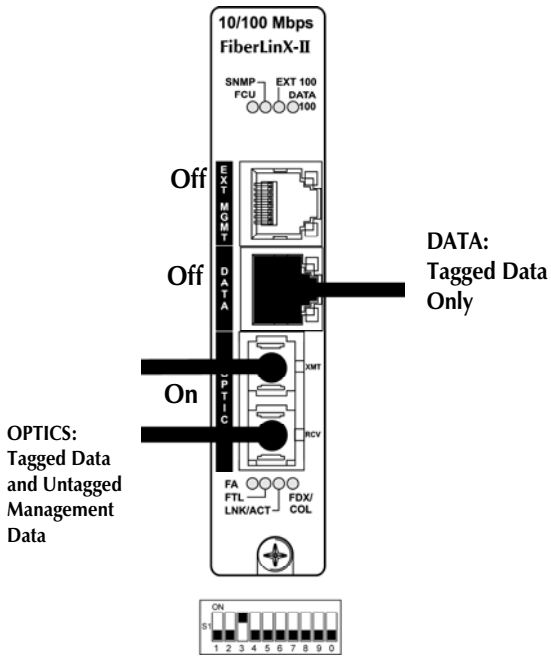
   d. Type **Reboot**. In this mode only tagged data will pass to the data port.

NOTE
The flow of management domain traffic is defined by the DIP Switches. For example, if the management DIP Switches are on the OPTICS and DATA ports, management domain traffic is allowed to flow through those ports.

External Management is ON



External Management is OFF

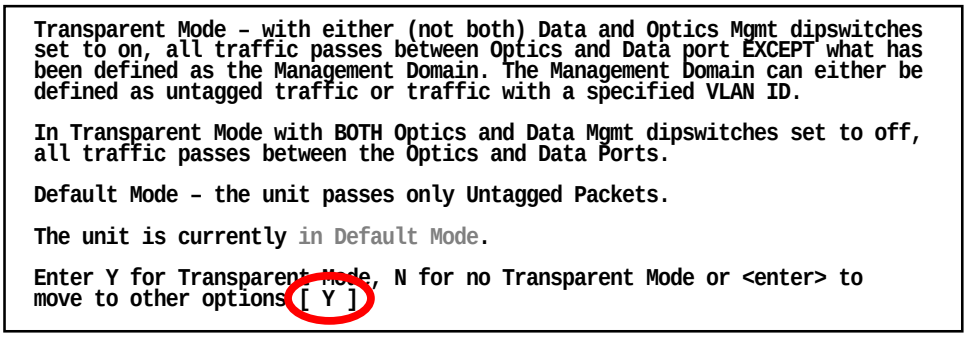


Mode Three-Transparency with Tagged Management

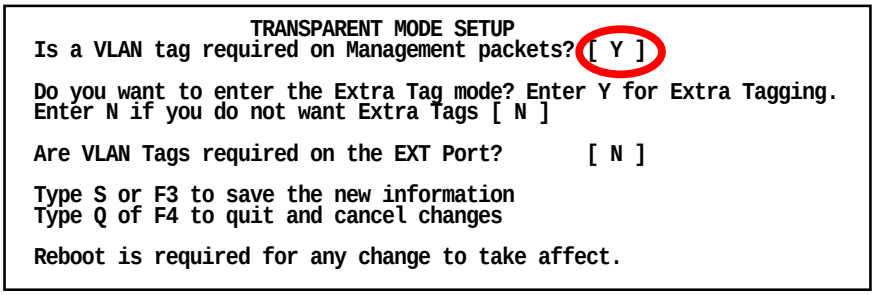
Transparent with Tagged Management mode passes both tagged and untagged traffic between the DATA port and the OPTICS (or UPLINK) port. By using a VLAN Tag, it is possible to isolate and route the management path in the module. This method can be used with or without continuing the management path down the EXT MGMT port.

To configure this mode, do the following:

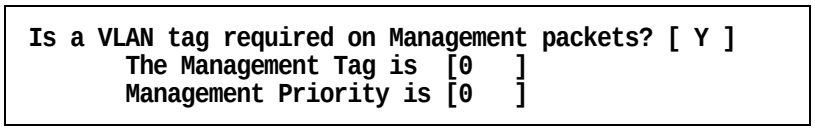
1. Set the management DIP Switch ON for the ports using management (in this example it is the OPTICS (or UPLINK) 3 = ON and EXT MGMT 1 = ON).
2. Set Transparent Mode to allow both tagged and untagged traffic to pass:
   a. In the Main Configuration screen, press the **Space Bar** and type **config**. The Configuration screen displays:


Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches set to on, all traffic passes between Optics and Data port EXCEPT what has been defined as the Management Domain. The Management Domain can either be defined as untagged traffic or traffic with a specified VLAN ID.
In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off, all traffic passes between the Optics and Data Ports.
Default Mode – the unit passes only Untagged Packets.
The unit is currently in Default Mode.
Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to move to other options [Y]

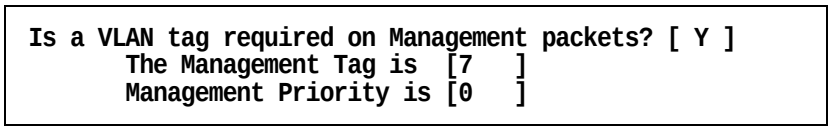
   b. Enter **Y** in the Transparent Mode field and press any key (except S or Q) to open the Transparent Mode Setup screen.


TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [Y]
Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [N]
Are VLAN Tags required on the EXT Port? [N]
Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes
Reboot is required for any change to take affect.

   c. Enter Y at **Is a VLAN tag required on Management packets?** The screen displays the management tag fields:



   d. Enter the management tag (VLAN ID) and the priority (optional).

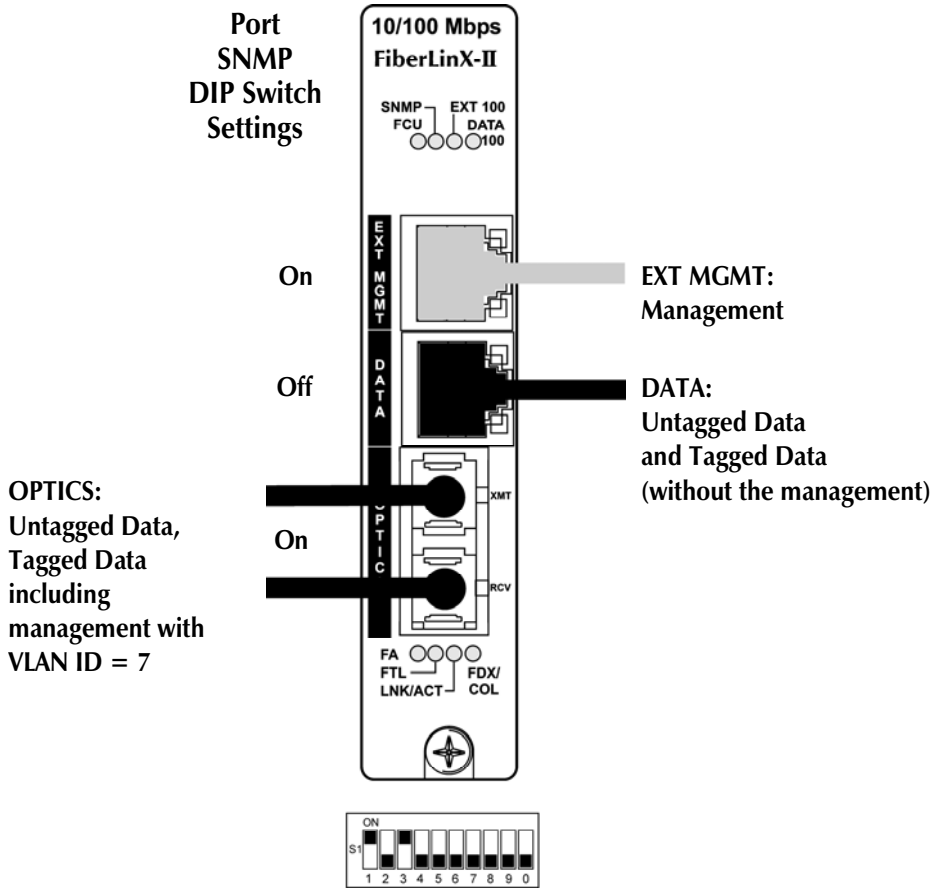


e. Ensure **Are VLAN Tags required on the EXT Port?** is set to N.

f. Press **S** or **F3** to save the settings. This will set all traffic with VLAN ID 7 as management.

g. Type **Reboot**.

Now the iMcV-FiberLinX-II is configured to pass all data between the OPTICS (or UPLINK) and DATA ports except that which is tagged with VLAN ID 7. All data tagged with VLAN ID 7 is considered management traffic and passes from the OPTICS (or UPLINK) port to the EXT MGMT port only. The iMcV-FiberLinX-II is configured to receive untagged data from the twisted pair EXT MGMT port and add the VLAN ID 7 before sending it out of the OPTICS (or UPLINK) port. In this mode the EXT MGMT port provides a secure link to the management port at the other end of the fiber line.



EXT MGMT and OPTICS (or UPLINK)
Port Management DIP Switches 1 & 3 set to ON.

Mode Four-Transparency with Extra Tagging (Q-in-Q)

Transparent with Extra Tagging mode can add an extra tag to data received on the DATA port. By using Extra Tagging in a Host/Remote iMcV-FiberLinX-II pair, all data

received on the Remote iMcV-FiberLinX-II DATA port can be extra-tagged and sent out of the Host iMcV-FiberLinX-II DATA port with a unique tag for identification in the Host cloud. In the reverse direction the extra tag is removed before sending the data out of the Remote iMcV-FiberLinX-II DATA port.

To configure this mode, perform the following:

Set the Extra Tag Mode on both of the iMcV-FiberLinX-II modules:

1. In the Main Configuration screen, press the **Space Bar** and type **config**. The Configuration screen displays:

```
Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches
set to on, all traffic passes between Optics and Data port EXCEPT what has
been defined as the Management Domain. The Management Domain can either be
defined as untagged traffic or traffic with a specified VLAN ID.

In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off,
all traffic passes between the Optics and Data Ports.

Default Mode – the unit passes only Untagged Packets.

The unit is currently in Default Mode.

Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to
move to other options [ Y ]
```

2. Enter **Y** in the Transparent Mode field and press any key (except S or Q) to open the Transparent Mode Setup screen.

```
                    TRANSPARENT MODE SETUP
Is a VLAN tag required on Management packets? [ Y ]

Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ N ]

Are VLAN Tags required on the EXT Port?       [ N ]

Type S or F3 to save the new information
Type Q of F4 to quit and cancel changes

Reboot is required for any change to take affect.
```

3. Enter **Y** when prompted with **Do you want to enter the Extra Tag mode?** The screen expands to displays the Extra Tag mode fields:

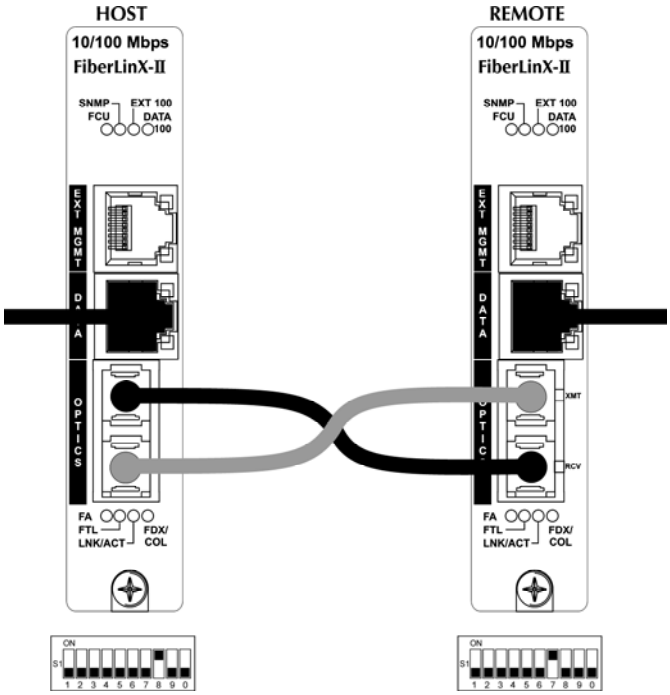
```
Do you want to enter the Extra Tag mode? Enter Y for Extra Tagging.
Enter N if you do not want Extra Tags [ Y ]
       The Data Tag is         [0   ]
       Data Priority is        [0   ]
Are Extra Tags left on the Data Port?         [ N ]

Select the TPID for the Extra Tag   1 = 8100, 2 = 9100, 3 = 9200
       Extra Tag TPID [ 1 ]   [8100]
```

Enter the extra tag VLAN ID (for example, 8), the Priority (optional), and the EtherType (optional). These values must be identical on both iMcV-FiberLinX-II modules.

```
       The Data Tag is         [8   ]
       Data Priority is        [0   ]
Are Extra Tags left on the Data Port?          [ N ]

Select the TPID for the Extra Tag   1 = 8100, 2 = 9100, 3 = 9200
       Extra Tag TPID [ 1 ]   [8100]
```

4. On the Host iMcV-FiberLinX-II module, enter **Y** at **Are Extra Tags left on the Data Port?** to only accept the Extra Tag VLAN ID on the DATA port. On the Remote iMcV-FiberLinX-II module, enter **N** to have the Extra Tag VLAN ID added to incoming and removed from outgoing data on the DATA port.
5. Select the Extra Tag TPID EtherType (optional).
6. Press **S** or **F3** to save the settings.
7. Type **Reboot**. Repeat steps for second module.

Now the iMcV-FiberLinX-II Host/Remote pair is configured to pass only VLAN ID 8 data from the Host iMcV-FiberLinX-II to the Remote iMcV-FiberLinX-II where the VLAN ID 8 tag is removed before sending the data out of the Remote DATA port. The Extra Tag VLAN ID 8 is added to all data received on the Remote DATA port before being sent to the Host iMcV-FiberLinX-II where the VLAN ID 8 tag remains on the data leaving the Host DATA port.



HOST DATA: Untagged and Tagged Data wrapped in Extra Tag of VLAN ID=8

REMOTE DATA: Untagged and Tagged Data

Host DIP Switch (8) set to ON

Remote DIP Switch (7) set to ON

Mode Five-Port VLAN

The Port VLAN mode allows configuring the iMcV-FiberLinX-II to accept only data tagged with one specific VLAN ID. This mode can be configured for either the OPTICS (or UPLINK) port or the DATA port.

VLAN on DATA Port - Configuration

To configure this mode, perform the following:

1. In the Main Configuration screen, press the **Space Bar** and type **config**. The Configuration screen displays:

```
Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches
set to on, all traffic passes between Optics and Data port EXCEPT what has
been defined as the Management Domain. The Management Domain can either be
defined as untagged traffic or traffic with a specified VLAN ID.

In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off,
all traffic passes between the Optics and Data Ports.

Default Mode – the unit passes only Untagged Packets.

The unit is currently in Default Mode.

Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to
move to other options [ N ]
```

2. Enter **N** in the Transparent Mode field and press any key (except S or Q) to open the VLAN screen:

```
Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.

          VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
 Ports                                        Data VLANs are used only
 Optics  [0   ]   [0   ]    [0  ]   [0  ]   [ N ]  if Tags are enabled on both
 Data    [0   ]   [0   ]    [0  ]   [0  ]   [ N ]  the Optics and Data Ports.
 Management VLAN                        EXT Mgmt Tag
 SNMP    [0   ]   [0   ]    [0  ]   [0  ]   [ N ]

 Data VLANs  <Optics <----> Data>
 VLAN  1 [0   ]   [0   ]  VLAN 12 [0   ]   [0   ]   VLAN 23 [0   ]   [0   ]
 VLAN  2 [0   ]   [0   ]  VLAN 13 [0   ]   [0   ]   VLAN 24 [0   ]   [0   ]
 VLAN  3 [0   ]   [0   ]  VLAN 14 [0   ]   [0   ]   VLAN 25 [0   ]   [0   ]
 VLAN  4 [0   ]   [0   ]  VLAN 15 [0   ]   [0   ]   VLAN 26 [0   ]   [0   ]
 VLAN  5 [0   ]   [0   ]  VLAN 16 [0   ]   [0   ]   VLAN 27 [0   ]   [0   ]
 VLAN  6 [0   ]   [0   ]  VLAN 17 [0   ]   [0   ]   VLAN 28 [0   ]   [0   ]
 VLAN  7 [0   ]   [0   ]  VLAN 18 [0   ]   [0   ]   VLAN 29 [0   ]   [0   ]
 VLAN  8 [0   ]   [0   ]  VLAN 19 [0   ]   [0   ]   VLAN 30 [0   ]   [0   ]
 VLAN  9 [0   ]   [0   ]  VLAN 20 [0   ]   [0   ]   VLAN 31 [0   ]   [0   ]
 VLAN 10 [0   ]   [0   ]  VLAN 21 [0   ]   [0   ]   VLAN 32 [0   ]   [0   ]
 VLAN 11 [0   ]   [0   ]  VLAN 22 [0   ]   [0   ]
Valid VLAN IDs are between 1 and 4094. Valid priorities are between 0 and 7.
Type S or F3 to save the changes. Type Q or F4 to quit and cancel changes.
```

3. Enter **Y** in the Tags column of the Data row and enter a VLAN ID in the VLAN IDs Current column of the OPTICS row (for example, 13).

```
          VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
 Ports
 Optics  [0   ]   [13  ]    [0  ]   [0  ]   [ N ]
 Data    [0   ]   [0   ]    [0  ]   [0  ]   [ Y ]
```

Data VLANs are used only if Tags are enabled on both the Optics and Data Ports.

Enter a VLAN ID in the **Management VLAN** IDs field.

```
          VLAN IDs          Priorities      Tags
       Current   Saved    Current   Saved
Ports
Optics  [0   ]   [13  ]    [0  ]    [0  ]   [ N ]
Data    [0   ]   [0   ]    [0  ]    [0  ]   [ Y ]
Management VLAN.....................EXT Mgmt Tag
SNMP....[0   ]   [20  ]    [0  ]    [0  ]   [ Y ]
```

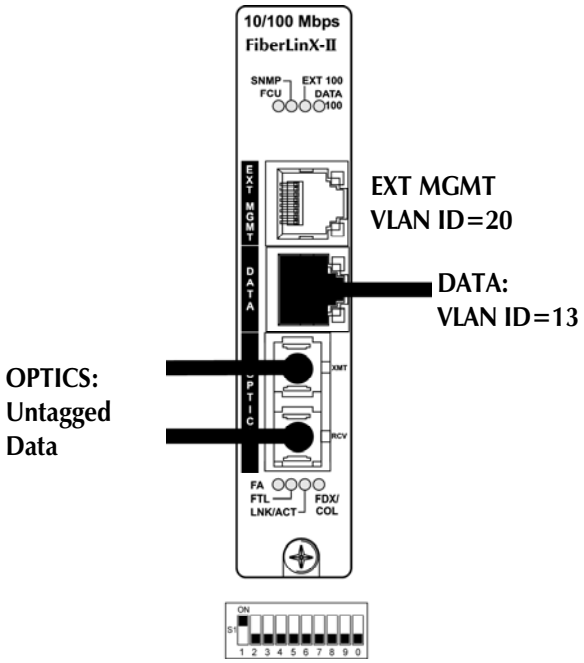
Data VLANs are used only if Tags are enabled on both the Optics and Data Ports.

4. Press **S** or **F3** to save the settings.

5. Type **Reboot**.

Now the iMcV-FiberLinX-II is configured to pass only VLAN ID 13 from the DATA port to the OPTICS (or UPLINK) port. Untagged packets arriving at the OPTICS (or UPLINK) port (Tags = N) receive a tag (VLAN ID = 13) before being sent out of the DATA port. The VLAN ID number used for a port must be different than the number used for the Management VLAN ID tag (VLAN ID=20). The EXT MGMT must have VLAN=20.

If **Y** is entered in the EXT MGMT Tag field, the VLAN ID for this port is the value in the Management VLAN field. In this case, define a VLAN ID in the Management VLAN field. If the unit is managed through the EXT MGMT port using untagged frames, the Management VLAN does not need to be defined.



EXT MGMT Port Management DIP Switch 1 set to ON.

VLAN on OPTIC Port - Configuration

To configure this mode, do the following:

1. In the Main Configuration screen, press the **Space Bar** and type **config**. The Configuration screen displays:

```
Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches
set to on, all traffic passes between Optics and Data port EXCEPT what has
been defined as the Management Domain. The Management Domain can either be
defined as untagged traffic or traffic with a specified VLAN ID.

In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off,
all traffic passes between the Optics and Data Ports.

Default Mode – the unit passes only Untagged Packets.

The unit is currently in Default Mode.

Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to
move to other options [ N ]
```

2. Enter **N** in the Transparent Mode field and press any key (except S or Q) to open the VLAN screen:

```
Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.

           VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
 Ports                                          Data VLANs are used only
 Optics  [0   ]   [0   ]    [0  ]    [0  ]   [ N ]  if Tags are enabled on both
 Data    [0   ]   [0   ]    [0  ]    [0  ]   [ N ]  the Optics and Data Ports.
 Management VLAN                          EXT Mgmt Tag
 SNMP    [0   ]   [0   ]    [0  ]    [0  ]   [ N ]

 Data VLANs  <Optics <----> Data>
 VLAN  1 [0   ]   [0   ]  VLAN 12 [0   ]   [0   ]   VLAN 23 [0   ]   [0   ]
 VLAN  2 [0   ]   [0   ]  VLAN 13 [0   ]   [0   ]   VLAN 24 [0   ]   [0   ]
 VLAN  3 [0   ]   [0   ]  VLAN 14 [0   ]   [0   ]   VLAN 25 [0   ]   [0   ]
 VLAN  4 [0   ]   [0   ]  VLAN 15 [0   ]   [0   ]   VLAN 26 [0   ]   [0   ]
 VLAN  5 [0   ]   [0   ]  VLAN 16 [0   ]   [0   ]   VLAN 27 [0   ]   [0   ]
 VLAN  6 [0   ]   [0   ]  VLAN 17 [0   ]   [0   ]   VLAN 28 [0   ]   [0   ]
 VLAN  7 [0   ]   [0   ]  VLAN 18 [0   ]   [0   ]   VLAN 29 [0   ]   [0   ]
 VLAN  8 [0   ]   [0   ]  VLAN 19 [0   ]   [0   ]   VLAN 30 [0   ]   [0   ]
 VLAN  9 [0   ]   [0   ]  VLAN 20 [0   ]   [0   ]   VLAN 31 [0   ]   [0   ]
 VLAN 10 [0   ]   [0   ]  VLAN 21 [0   ]   [0   ]   VLAN 32 [0   ]   [0   ]
 VLAN 11 [0   ]   [0   ]  VLAN 22 [0   ]   [0   ]
Valid VLAN IDs are between 1 and 4094. Valid priorities are between 0 and 7.
Type S or F3 to save the changes. Type Q or F4 to quit and cancel changes.
```

3. Enter **Y** in the Tags column of the Optics row and enter a VLAN ID in the VLAN IDs Current column of the Data row (for example, 13).

```
           VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
 Ports
 Optics  [0   ]   [0   ]    [0  ]    [0  ]   [ Y ]
 Data    [0   ]   [13  ]    [0  ]    [0  ]   [ N ]
```

Data VLANs are used only if Tags are enabled on both the Optics and Data Ports.

4. Enter a VLAN ID in the **Management VLAN** IDs field.

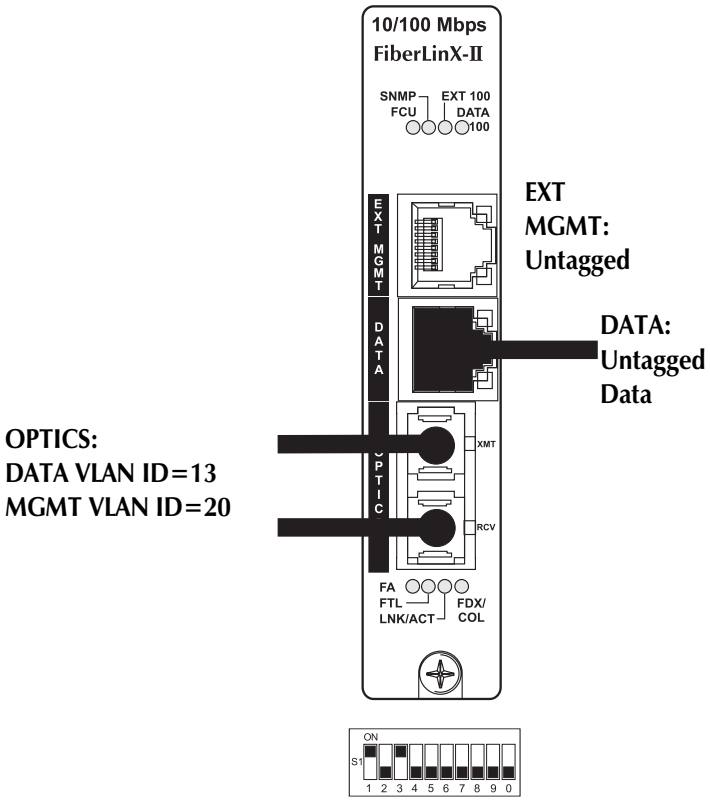
```
          VLAN IDs          Priorities     Tags
       Current   Saved    Current   Saved
Ports
Optics  [0   ]   [13  ]    [0  ]    [0  ]   [ N ]
Data    [0   ]   [0   ]    [0  ]    [0  ]   [ Y ]
Management VLAN.....................EXT Mgmt Tag
SNMP....[0   ]   [20  ]    [0  ]    [0  ]   [ N ]
```

   Data VLANs are used only if Tags are enabled on both the Optics and Data Ports.

5. Press **S** or **F3** to save the settings.

6. Type **Reboot**.

Now the iMcV-FiberLinX-II is configured to pass only VLAN ID 13 from the OPTICS (or UPLINK) port to the DATA port. Untagged packets arriving at the DATA port (Tags = N) receive a tag (VLAN ID = 13) before being sent out of the OPTICS (or UPLINK) port. The VLAN ID number used for a port must be different than the number used for the Management VLAN ID.



EXT MGMT Port Management DIP Switches 1 & 3 Set to ON.

Management of a host unit through the external port requires an IP address on the host unit. A remote unit connected over the fiber link is managed through the local unit using internal IP-less communication. If direct IP management of remote units is required, then DIP Switch #3 must be ON and the remote must have an IP address.

Mode Six-Port VLAN Filter

The VLAN filter mode allows isolating a segment of the network to only accept data using some or all of the 32 available VLAN IDs.

To configure this mode, do the following:

1. In the Main Configuration screen, press the **Space Bar** and type **config**. The Configuration screen displays:

```
Transparent Mode – with either (not both) Data and Optics Mgmt dipswitches
set to on, all traffic passes between Optics and Data port EXCEPT what has
been defined as the Management Domain. The Management Domain can either be
defined as untagged traffic or traffic with a specified VLAN ID.

In Transparent Mode with BOTH Optics and Data Mgmt dipswitches set to off,
all traffic passes between the Optics and Data Ports.

Default Mode – the unit passes only Untagged Packets.

The unit is currently in Default Mode.

Enter Y for Transparent Mode, N for no Transparent Mode or <enter> to
move to other options [ N ]
```

2. Enter **N** in the Transparent Mode field and press any key (except S or Q) to open the VLAN screen:

```
Saved VLAN Values <Active after reboot>. Current VLAN Values <Active now>.

           VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
Ports                                          Data VLANs are used only
Optics  [0   ]   [0   ]    [0  ]    [0  ]   [ N ]  if Tags are enabled on both
Data    [0   ]   [0   ]    [0  ]    [0  ]   [ N ]  the Optics and Data Ports.
Management VLAN                          EXT Mgmt Tag
SNMP    [0   ]   [0   ]    [0  ]    [0  ]   [ N ]

Data VLANs  <Optics <----> Data>
VLAN  1 [0   ]   [0   ]  VLAN 12 [0   ]   [0   ]   VLAN 23 [0   ]   [0   ]
VLAN  2 [0   ]   [0   ]  VLAN 13 [0   ]   [0   ]   VLAN 24 [0   ]   [0   ]
VLAN  3 [0   ]   [0   ]  VLAN 14 [0   ]   [0   ]   VLAN 25 [0   ]   [0   ]
VLAN  4 [0   ]   [0   ]  VLAN 15 [0   ]   [0   ]   VLAN 26 [0   ]   [0   ]
VLAN  5 [0   ]   [0   ]  VLAN 16 [0   ]   [0   ]   VLAN 27 [0   ]   [0   ]
VLAN  6 [0   ]   [0   ]  VLAN 17 [0   ]   [0   ]   VLAN 28 [0   ]   [0   ]
VLAN  7 [0   ]   [0   ]  VLAN 18 [0   ]   [0   ]   VLAN 29 [0   ]   [0   ]
VLAN  8 [0   ]   [0   ]  VLAN 19 [0   ]   [0   ]   VLAN 30 [0   ]   [0   ]
VLAN  9 [0   ]   [0   ]  VLAN 20 [0   ]   [0   ]   VLAN 31 [0   ]   [0   ]
VLAN 10 [0   ]   [0   ]  VLAN 21 [0   ]   [0   ]   VLAN 32 [0   ]   [0   ]
VLAN 11 [0   ]   [0   ]  VLAN 22 [0   ]   [0   ]
Valid VLAN IDs are between 1 and 4094. Valid priorities are between 0 and 7.
Type S or F3 to save the changes. Type Q or F4 to quit and cancel changes.
```

3. Enter **Y** in the Tags column of both the Optics row and the Data row to enable Data VLANs.

```
           VLAN IDs          Priorities     Tags
        Current   Saved    Current   Saved
Ports
Optics  [0   ]   [0   ]    [0  ]    [0  ]   [ Y ]
Data    [0   ]   [0   ]    [0  ]    [0  ]   [ Y ]
```

Data VLANs are used only if Tags are enabled on both the Optics and Data Ports.

4. Enter a VLAN ID in the **Management VLAN** IDs field.

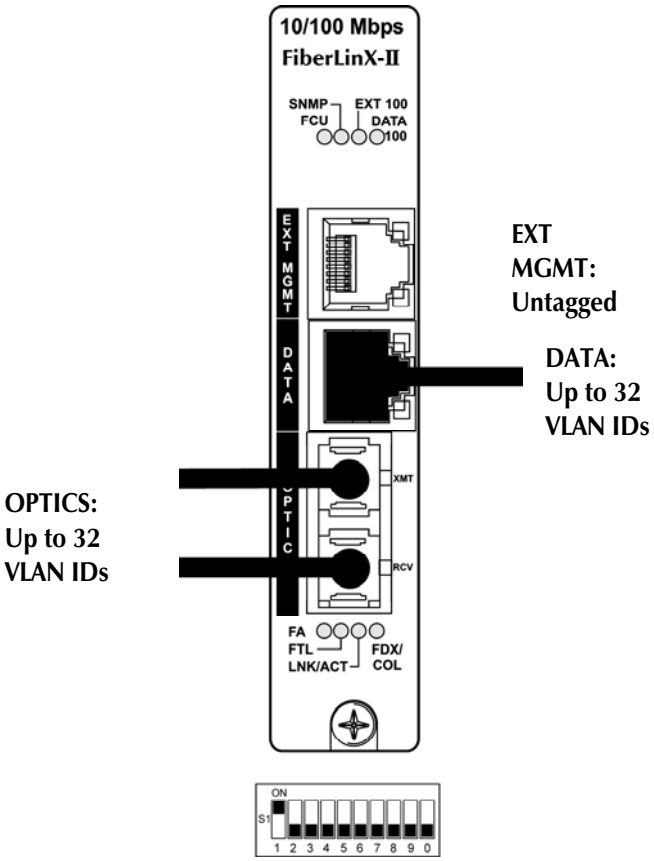
Enter up to 32 VLAN IDs in the Data VLANs rows. VLAN IDs can range from 1 to 4094.

```
Data VLANs  <Optics <----> Data>
VLAN  1 [0   ]   [101 ]  VLAN 12 [0   ]   [112 ]   VLAN 23 [0   ]   [123 ]
VLAN  2 [0   ]   [102 ]  VLAN 13 [0   ]   [113 ]   VLAN 24 [0   ]   [124 ]
VLAN  3 [0   ]   [103 ]  VLAN 14 [0   ]   [114 ]   VLAN 25 [0   ]   [125 ]
VLAN  4 [0   ]   [104 ]  VLAN 15 [0   ]   [115 ]   VLAN 26 [0   ]   [126 ]
VLAN  5 [0   ]   [105 ]  VLAN 16 [0   ]   [116 ]   VLAN 27 [0   ]   [127 ]
VLAN  6 [0   ]   [106 ]  VLAN 17 [0   ]   [117 ]   VLAN 28 [0   ]   [128 ]
VLAN  7 [0   ]   [107 ]  VLAN 18 [0   ]   [118 ]   VLAN 29 [0   ]   [129 ]
VLAN  8 [0   ]   [108 ]  VLAN 19 [0   ]   [119 ]   VLAN 30 [0   ]   [130 ]
VLAN  9 [0   ]   [109 ]  VLAN 20 [0   ]   [120 ]   VLAN 31 [0   ]   [131 ]
VLAN 10 [0   ]   [110 ]  VLAN 21 [0   ]   [121 ]   VLAN 32 [0   ]   [132 ]
VLAN 11 [0   ]   [111 ]  VLAN 22 [0   ]   [122 ]
```

5. Press **S** or **F3** to save the settings.

6. Type **Reboot**.

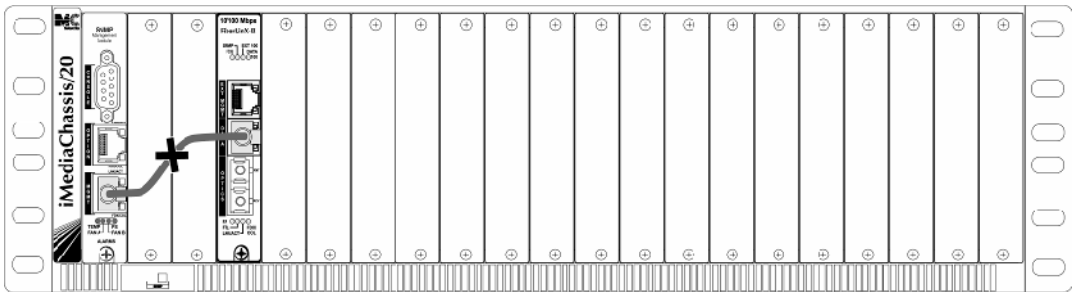
Now the iMcV-FiberLinX-II is configured to pass only packets with tags containing the VLAN IDs defined in the Data VLANs table. VLAN ID numbers defined in this table must not be the same as the number used for the Management VLAN ID.



EXT MGMT port management DIP Switch 1 set to ON.

- If two iMcV-FiberLinX-II Host/Remote units are not communicating properly, make sure one is a Host and the other is a Remote. If the second unit is not configured as a Remote, it will be recognized as a Standalone unit and the Host and Remote units will not communicate with each other properly. Setting the OPTICS (or UPLINK) port management DIP Switch #3 to the ON position on both modules will allow performing a simple ping test. This is possible only if pinging from the computer through the optics uplink port, which is highly unusual. The EXT or data switch must be enabled and connected to the computer to ping either device.
- If a link on a twisted pair port cannot be established, make sure the cable is in working order; if not, replace the cable (iMcV-FiberLinX-II includes AutoCross; a link should be detected regardless of the Cat5 cable type).
- If a fiber link cannot be established, make sure that the fiber transceivers on iMcV-FiberLinX-II are not over/under driving the fiber receivers. For fiber specifications, please visit www.imcnetworks.com/support/fpblookup.cfm. Make sure the fiber mode and wavelength on both iMcV-FiberLinX-II units match (i.e., both are 1310 nm single-mode fiber).
- Make sure the port speeds on iMcV-FiberLinX-II match those on the end devices connected to iMcV-FiberLinX-II. IMC Networks recommends configuring all connected devices to Auto Negotiation, or if using Force mode, ensure speed and duplex settings match.
- If using single-strand fiber, make sure the pair of devices is compatible single-strand fiber devices. For example, an iMcV-FiberLinX-II TX/SSFX-SM1310-SC which transmits 1310 nm and receives 1550 nm must be connected to a device which transmits 1550 nm and receives 1310 nm.
- If using an iMcV-FiberLinX-II unit with an SFP port and it is not functioning properly or at all, make sure that the installed SFP module is the correct speed (100 Mbps).
- When using the FiberAlert feature, make sure that FiberAlert is enabled on only one unit when connecting two iMcV-FiberLinX-II units, or when connecting an iMcV-FiberLinX-II to another IMC Networks media converter which includes the FiberAlert feature.
- If management is not functioning properly, make sure that the DIP Switch settings are accurate for the port to be managed.

- To restore the unit to factory default settings, use the cleandb function via the serial port (refer to the Device-Specific Options from the Command Line section for more information). This is especially helpful if the module may have been configured improperly. If restarting to factory defaults is necessary, IMC Networks recommends using this function on both units in Host/Remote applications, then reconfiguring all settings.
- Ensure READ/WRITE Community Strings for iMcV-FiberLinX-II and iView^2 are the same.



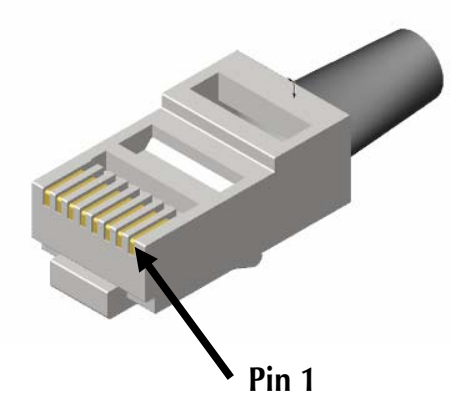
- Ensure none of the twisted-pair ports on the iMcV-FiberLinX-II are connected to the twisted-pair port on the iMediaCenter chassis or the management module in an iMediaChassis series chassis.

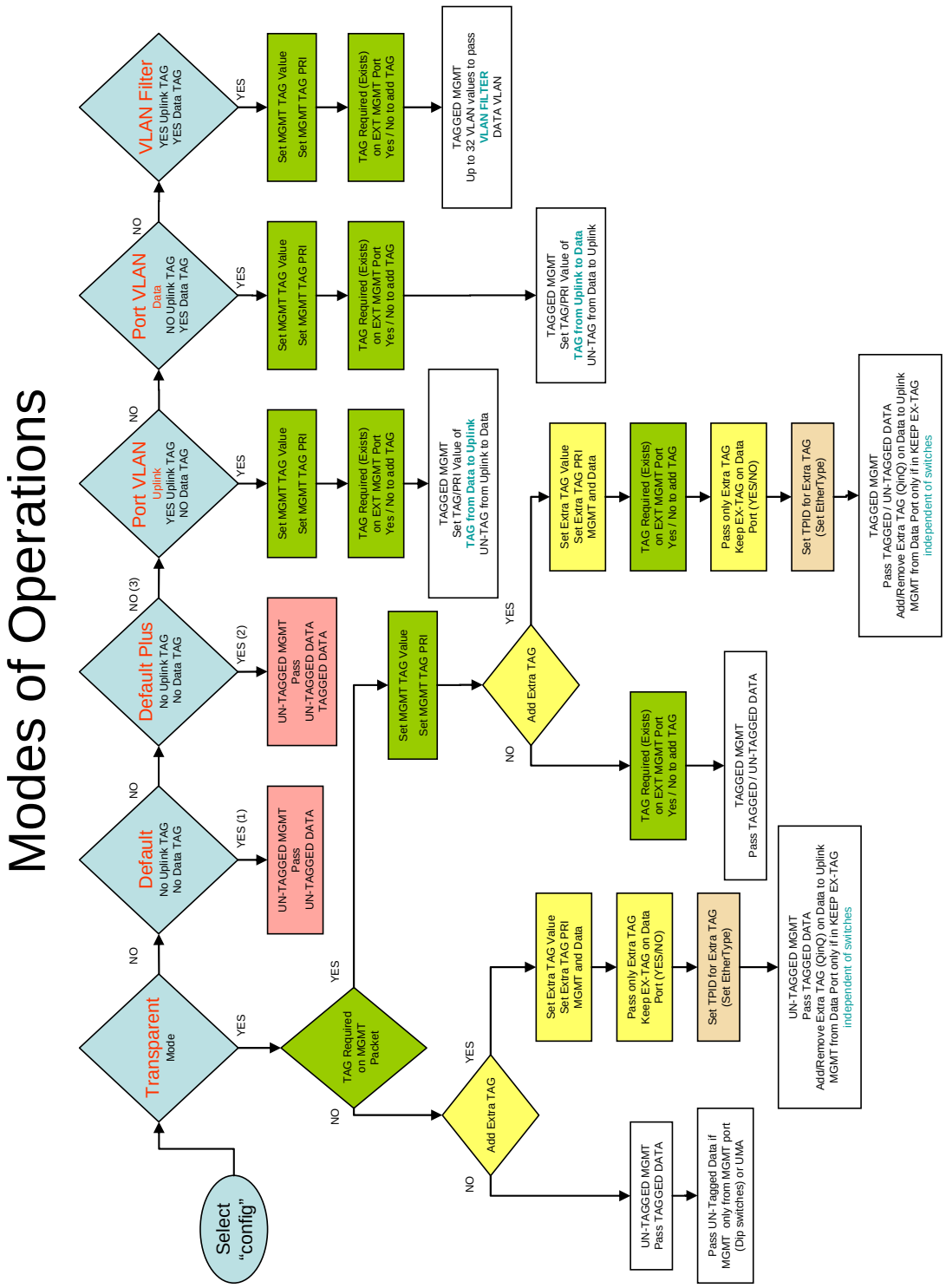
Serial Port Pinout

The following table lists the pin configuration for the RJ-45/Serial connector. The serial port shares the physical connector for the Ethernet port defined as external management (EXT MGMT).

*RS-232 signals are connected only on the EXT MGMT port.

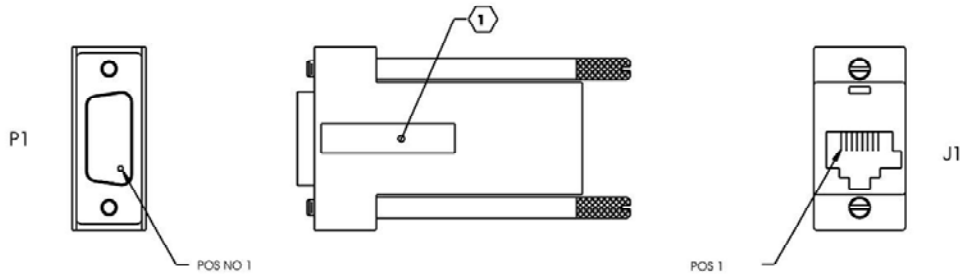
Pin	Signal
1	*Transmit +*
2	*Transmit -*
3	*Receive +*
4	*None*
5	*Transmit Serial**
6	*Receive -*
7	*Receive Serial**
8	*Ground Serial**

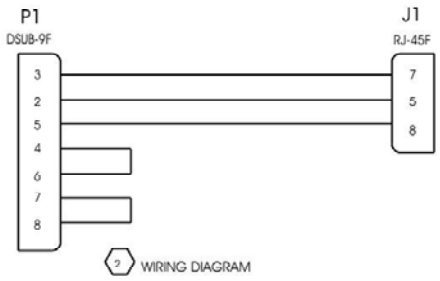



Modes of Operations
Select "config"
Transparent Mode
YES
NO
Default No Uplink TAG No Data TAG
YES (1)
NO
UN-TAGGED MGMT Pass UN-TAGGED DATA
Default Plus No Uplink TAG No Data TAG
YES (2)
NO (3)
UN-TAGGED MGMT Pass UN-TAGGED DATA TAGGED DATA
Port VLAN Uplink YES Uplink TAG NO Data TAG
YES
NO
Set MGMT TAG Value Set MGMT TAG PRI
TAG Required (Exists) on EXT MGMT Port Yes / No to add TAG
TAGGED MGMT Set TAG/PRI Value of TAG from Uplink to Data UN-TAG from Uplink to Data
Port VLAN Data NO Uplink TAG YES Data TAG
YES
NO
Set MGMT TAG Value Set MGMT TAG PRI
TAG Required (Exists) on EXT MGMT Port Yes / No to add TAG
TAGGED MGMT Set TAG/PRI Value of TAG from Uplink to Data UN-TAG from Data to Uplink
VLAN Filter YES Uplink TAG YES Data TAG
YES
Set MGMT TAG Value Set MGMT TAG PRI
TAG Required (Exists) on EXT MGMT Port Yes / No to add TAG
TAGGED MGMT Up to 32 VLAN values to pass VLAN FILTER DATA VLAN
TAG Required on MGMT Packet
YES
NO
Set MGMT TAG Value Set MGMT TAG PRI
Add Extra TAG
YES
NO
Set Extra TAG Value Set Extra TAG PRI MGMT and Data
Pass only Extra TAG Keep EX-TAG on Data Port (YES/NO)
Set TPID for Extra TAG (Set EtherType)
UN-TAGGED MGMT Pass TAGGED DATA Add/Remove Extra TAG (QinQ) on Data to Uplink MGMT from Data Port only if in KEEP EX-TAG independent of switches
Set Extra TAG Value Set Extra TAG PRI MGMT and Data
TAG Required (Exists) on EXT MGMT Port Yes / No to add TAG
Pass only Extra TAG Keep EX-TAG on Data Port (YES/NO)
Set TPID for Extra TAG (Set EtherType)
TAGGED MGMT Pass TAGGED / UN-TAGGED DATA
TAGGED MGMT Pass TAGGED / UN-TAGGED DATA Add/Remove Extra TAG (QinQ) on Data to Uplink MGMT from Data Port only if in KEEP EX-TAG independent of switches
UN-TAGGED MGMT Pass TAGGED DATA
Pass UN-Tagged Data if MGMT only from MGMT port (Dip switches) or UMA

Appendix

The listed products offer an optional method of configuring the device via a Console session by connecting an RJ-45 to DB9 adapter (see pertinent manuals for further information). The adapter is available for purchase through IMC Networks; the schematic included below will enable the end user to wire one of their own.





IMC Networks Technical Support

Tel: (949) 465-3000 or (800) 624-1070 (in the U.S. and Canada);

+32-16-550880 (Europe)

Fax: (949) 465-3020

E-Mail: techsupport@imcnetworks.com

Web: www.imcnetworks.com

Power Consumption (Typical):
0.850 A @ 3.6V DC max.

Operating Temperature:
32° to 122° F (0° to 50° C)

Storage Temperature:
0° to 160°F (-20° to 70° C)

Humidity:
5 to 95% (non-condensing); 0 to 10,000 ft. altitude

Dimensions:
Single Slot iMcV module

Standards/Compliance

- Read/write IEEE 802.1Q VLAN tags
- QoS IEEE 802.1p-based packet prioritization (2 queues [high/low] with 8 levels of priority
- IEEE 802.3x Flow Control
- IEEE 802.3i 10Base-T twisted pair
- IEEE 802.3u 100Base-TX twisted pair
- IEEE 802.3u 100Base-FX or SX fiber

Fiber Optic Cleaning Guidelines

Fiber Optic transmitters and receivers are extremely susceptible to contamination by particles of dirt or dust, which can obstruct the optic path and cause performance degradation. Good system performance requires clean optics and connector ferrules.

1. Use fiber patch cords (or connectors, as appropriate) only from a reputable supplier; low-quality components can cause many hard-to-diagnose problems in an installation.
2. Dust caps are installed at IMC Networks to ensure factory-clean optical devices. These protective caps should not be removed until the moment of connecting the fiber cable to the device. Should it be necessary to disconnect the fiber device, reinstall the protective dust caps.
3. Store spare caps in a dust-free environment such as a sealed plastic bag or box so that when reinstalled they do not introduce any contamination to the optics.
4. If it is suspected that the optics have been contaminated, alternate between blasting with clean, dry, compressed air and flushing with methanol to remove particles of dirt.

Electrostatic Discharge Precautions

Electrostatic discharge (ESD) can cause damage to any product, add-in modules or stand alone units containing electronic components. Always observe the following precautions when installing or handling these kinds of products

1. Do not remove unit from its protective packaging until ready to install.
2. Wear an ESD wrist grounding strap before handling any module or component. If the wrist strap is not available, maintain grounded contact with the system unit throughout any procedure requiring ESD protection.
3. Hold the units by the edges; do not touch the electronic components or gold connectors.
4. After removal, always place the boards on a grounded, static-free surface, ESD pad or in a proper ESD bag. Do not slide the modules or stand alone units over any surface.

WARNING! Integrated circuits and fiber optic components are extremely susceptible to electrostatic discharge damage. Do not handle these components directly unless you are a qualified service technician and use tools and techniques that conform to accepted industry practices.

Safety Certifications

UL/CUL: Listed to Safety of Information Technology Equipment, including Electrical Business Equipment.

CE: The products described herein comply with the Council Directive on Electromagnetic Compatibility (2004/108/EC) and the Council Directive on Electrical Equipment Designed for use within Certain Voltage Limits (2006/95/EC). Certified to Safety of Information Technology Equipment, Including Electrical Business Equipment. For further details, contact IMC Networks.

Class 1 Laser product, Luokan 1 Laserlaite,
Laser Klasse 1, Appareil A'Laser de Classe 1

European Directive 2002/96/EC (WEEE) requires that any equipment that bears this symbol on product or packaging must not be disposed of with unsorted municipal waste. This symbol indicates that the equipment should be disposed of separately from regular household waste. It is the consumer's responsibility to dispose of this and all equipment so marked through designated collection facilities appointed by government or local authorities. Following these steps through proper disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about proper disposal, please contact local authorities, waste disposal services, or the point of purchase for this equipment.

19772 Pauling • Foothill Ranch, CA 92610-2611 USA
TEL: (949) 465-3000 • FAX: (949) 465-3020
www.imcnetworks.com

ISO 9001:2008 REGISTERED

RoHS

Made in USA

© 2010 IMC Networks. All rights reserved.
The information in this document is subject to change without notice. IMC Networks assumes no responsibility for any errors that may appear in this document. iMcV-FiberLinX-II is a trademark of IMC Networks. Other brands or product names may be trademarks and are the property of their respective companies.

Document Number 56-80011-01 A1 **April 2010**